OFFICIAL GAZETTE

of the

COMMON MARKET FOR EASTERN AND SOUTHERN AFRICA (COMESA)

Volume 16

Issued on 15th October 2011

LEGAL AND GENERAL NOTICES

TABLE OF CONTENTS

IT IS HEREBY NOTIFIED that the COMESA Council of Ministers at its Thirtieth Meeting held on 15 October 2011 at Lilongwe, Malawi issued the following Legal and General Notices:

LEGAL AND GENERAL NOTICES

Legal and General Notices Issued by the Council

SIMPLIFIED TRADE REGIME (STR)

Decisions

1. **Council made the following decisions:**

(a) Endorsed the ministerial decisions on the Simplified Trade Regime; and

(b) Decided that best practices in the region should be used in further improving the STR in future reviews, in order to promote better harmonisation at the Tripartite level.

COMESA FUND MINISTERIAL COMMITTEE

The COMESA Infrastructure Fund (CIF)

Decisions

2. **Council made the following decisions:**

(a) Adopted the CIF 2011 work programme;

(b) Adopted the budget attached to the work programme;

(c) That the composition of the Board of Governors of the CIF comprising of Ministers of Finance of countries that have ratified and paid their contributions to the base fund of the COMESA Fund, with the proviso that the board of Governors may be modified to include investors into the CIF as appropriate;

(d) That the interim investment committee be constituted by Rwanda, Zimbabwe, Mauritius as the COMESA Fund Bureau plus Kenya and Zambia, with the proviso that for the smooth functioning of the governance structure, account will be taken to have a rotational system. In order to ensure continuity, at least two members would be maintained at each rotation;

(e) That transaction advisors should be recruited to assist with the capital raising process;

(f) Authorised the borrowing of US $528,550 from the Base Fund to meet the costs of recruiting the transaction advisors, and that this amount be repaid to the COMESA Fund from capital raised. The timing of the repayment will be determined by the CIF Board of Governors;

(g) That linkages should be established between the Climate Change Fund and the CIF;

(h) That Member States that had not made their contributions to the COMESA Fund do so;

(i) That the CEO should update and submit a priority pipeline of projects for floating and exploring financing for such projects under the Aid for Trade framework.

COMESA Adjustment Facility

Decisions

3. **Council made the following decisions:**

(a) That a meeting involving the National Authorising Officers (NAOs) be convened before the finalisation of the Mid Term Review (MTR); and

(b) The next call for submissions to access the resources of Regional Integration Support Mechanism (RISM) as amended by the rider be launched.

MINISTERS OF FINANCE AND CENTRAL BANK GOVERNORS

Regional Payment and Settlement System (REPSS)

Decisions

4. Council made the following decisions:

(a) Commended the Central Banks of Democratic Republic of Congo, Malawi, Mauritius, Rwanda, Sudan, Swaziland, Uganda and Zambia for having signed the REPSS Agreements and prefunded their accounts at the Bank of Mauritius;

(b) Mandated the Secretary General of COMESA to have REPSS included on the Tripartite Agenda for it to become a Tripartite Facility; and

(c) Mandated the Secretary General of COMESA and the Chairman of the COMESA Committee of Governors of Central Banks to engage China, India and The Cooperation Council for the Arab States of the Gulf (GCC) on joining REPSS.

Operationalisation of the COMESA Monetary Institute
Decisions

5. **Council made the following decisions:**

(a) Approved the principle of using the COMESA Monetary Institute as the Tripartite Institute for the three RECs;

(b) The findings of the study undertaken on the utilisation of CMI as a Tripartite Institution should be submitted to Senior Officials of Ministries of Finance and Central Banks of COMESA, the East African Community (EAC) and Southern Africa Development Community (SADC) for consideration and submission to the Tripartite Task Force; and

(c) Member States which had not signed the Charter of CMI and which had not contributed to the budget should do so by the end of August 2011.

Macroeconomic Convergence in COMESA Member Countries

Decisions

6. Council made the following decisions:

(a) In order to enhance the implementation of the Monetary Harmonisation Programme of COMESA, Member States should continue to move towards macro-economic convergence, which take into account poverty reduction strategies that target growth and equitable distribution of benefits of growth in order to achieve the Millennium Development Goals.

(b) COMESA, as current Chair of the Tripartite Task Force, should initiate discussions with EAC and SADC to make Monetary and Fiscal Policies Harmonization Programme a Tripartite Programme.

COMESA Multilateral Fiscal Surveillance Framework (MFSF)

Decisions

7. Council made the following decisions:

(a) With technical assistance from the African Development Bank (AfDB), a task force should be set up to flesh out the proposal on embedding trade integration with MFSF, and make appropriate recommendations;

(b) A convergence council should be established with joint membership of the Ministers of Finance and Governors of

Central Banks, and tasked with the responsibility of multilateral surveillance. The Council of Ministers, along with the Committee of Ministers of Finance, Committee of Ministers of Trade and the Committee of Central Bank Governors, should actively follow developments in their mandated areas of responsibility;

(c) An 'Excessive Slippages Procedure' as described in the report of the Ministers of Finance and Governors of Central Banks should be established as the heart of the MFSF;

(d) A fiscal unit should be established in the COMESA Secretariat to service the Convergence Council;

(e) A CoSWAP Facility to provide liquidity in case of financial crisis in a member country should be set up. Governors of the Central Banks will work out its modalities;

(f) Member States should prepare National Convergence Programmes (NCPs) that delineate their time-path and policies to achieve the convergence criteria in light of their own circumstances.

(g) The performance of each country for multilateral surveillance purposes, and the activation of ESP if needed, will be in comparison to the objectives and time path of those national programmes.

(h) Member States should be provided with technical support to strengthen their national Public Finance Management Systems to ensure proper implementation of NCPs;

(i) COMESA, with assistance from the African Development Bank (AfDB), should organise three sub-regional workshops in the COMESA region to familiarize local officials with the proposed system;

(j) COMESA should open discussions with SADC and EAC on the proposals contained in the report in the light of the agreement's harmonization objectives;

(k) The Secretary General should approach AfDB at the highest level to make the services available of a staff member/consultant responsible for the report to participate in the above mentioned sub-regional workshops and to assist in those discussions; and

(l) The COMESA Secretariat should request development partners' assistance for capacity building in sound economic management in collaboration with the Regional Multi-Disciplinary Centre of Excellence (RMCE).

The COMESA Common Market Levy and other means of Financing Methods

Decisions

8. Council made the following decisions:

(a) The proposal for the COMESA Common Market Levy and other Financing Methods be reviewed and improved by the Secretariat for circulation and consideration by Member States. Such improvement should include a comparative analysis of the different options and their impact on the economies of the Member States; and Member States be involved in doing their own simulations;

(b) Member States should undertake more consultations on the innovative financing levies;

(c) A task force consisting of the fiscal affairs experts be established to consider and enhance the proposal before consideration by the Ministers in 2012; and

(d) The Secretariat should place the issues of innovative means of financing on the Programme for the Tripartite meetings.

The Regional Multi-Disciplinary Centre of Excellence (RMCE)

Decision

9. **Council made the following decision:**

(a) That the Secretariat should support the RMCE in the mobilisation of additional resources including in the context of the forthcoming review of the Intra-Africa Caribbean Pacific programme under the Tenth European Development Fund.

Growth and Economic Transformation in the Tripartite Region

Decisions

10. Council made the following decisions:

(a) Supported the policy package of reforms sketched out in the proposed road map for accelerated economic transformation in Eastern and Southern Africa, noting that financial market integration as well as real market integration are intertwined and an integral part of the monetary integration process.

(b) Mandated the COMESA Secretariat to formulate a detailed programme of the proposed reforms in close consultation and collaboration with Member States.

(c) The detailed programme should outline the specific reforms required pillar by pillar and on a country by country basis as well as the required and likely sources of funding and, the implementation and monitoring arrangements;

(d) Adopted the road map for accelerating economic transformation in Eastern and Southern Africa;

(e) That the proposal should be submitted for consideration by the other regional, economic communities of the Tripartite, that is the (East African Community and the Southern Africa Development Community;

(f) Recommended the full involvement of the private sector throughout the implementation of the five pillars and especially in identifying the barriers to doing business in Eastern and Southern Africa; and

(g) That the proposed road map for accelerated economic transformation in Eastern and Southern Africa should have a maximum of a five-year time line.

Establishment of the COMESA, EAC and SADC Tripartite Free Trade Area

Decision

11. Council made the following decision:

(a) That the various committees and policy organs of COMESA be continuously provided with reports being made under the Tripartite arrangement and programmes.

Regional Dimension of Aid Effectiveness

Decisions

12. **Council made the following decisions:**

(a) With respect to the Organisation for Economic Co-operation and Development (OECD) Working Party on Aid Effectiveness (WP-EFF) meeting, Busan Outcome Document (BOD), the African Caribbean and Pacific Group(ACP), and Africa/The New Partnership for Africa's Development (NEPAD), the next steps ahead should be:

i) To reaffirm that willing, regional organisations become signatories to the Paris Declaration principles;

ii) The Secretariat should, through the Inter-Regional Committee on Cooperation (IRCC) mechanism, closely follow-up the new drafts of the BOD to verify due inclusion of the COMESA/IRCC proposal in the run up to the final October preparatory meeting for Busan Fourth High Level Forum;

iii) The Secretariat and IRCC should continue work on the regional organisations position paper/regional organisations declaration associating the concepts of regional aid effectiveness with climate change financing, private sector involvement; leveraging, blending, fragile states; peace building; and conflict prevention issues;

iv) To invite the OECD WP-EFF Co-Chairs to the COMESA Summit in October 2011;

v) The Secretariat should participate in AUC/NPCA and ADB stakeholders' meeting on the African position paper for Busan that should also include reference to the COMESA/IRCC initiative to recognise the regional dimension;

vi) The Secretariat should prepare for high level participation in the October meeting and for ministerial/CEOs participation in Busan HLF IV.

vii) The Secretariat should, by 15 August 2011, prepare a draft action plan with timelines for circulation to Member States. On the basis of comments received, the Secretariat should produce a final work plan with indicative timelines by 15 September 2011.

Regularity of Meetings

Decision

13. **Council made the following decision:**

(a) That the next joint meeting of the Ministers of Finance and Governors of Central Banks should be held within the next twelve months.

AGRICULTURE, ENVIRONMENT AND NATURAL RESOURCES

Climate Change Initiative

Decisions

14. Council made the following decisions:

(a) That the ministers of agriculture should proactively engage in the ongoing climate change discussions in the period up to, during and beyond the 17th Session of the Conference of the Parties (COP 17) to ensure a decision is reached on agriculture, which is responsive to the African situation;

(b) That Member States should include agricultural experts in their multi-disciplinary climate change negotiation teams and ensure consistency; adequate negotiations skills and logistical support.

(c) The COMESA Secretariat, in collaboration with other Regional Economic Communities (RECs) and non state actors, should facilitate the consolidation of and championing of the unified African position;

(d) That Member States should actively engage in and support the up-scaling of climate smart agriculture;

(e) The COMESA Secretariat, in collaboration with relevant partners, should support Member States to set up legal and institutional frameworks necessary for effective participation in climate response measures (such as COMESA Carbon Fund, African Climate Fund, the United Nations Framework Convention on Climate Change (UNFCCC), Green Climate Fund and Fast Start Finance under the Copenhagen Accord); and

(f) The COMESA Secretariat should explore the possibility of setting up a centre of excellence on climate smart agriculture for the arid and semi-arid areas - to be based in Djibouti.

Sanitary and Phyto-sanitary (SPS) Programme in the COMESA Region

Decisions

15. Council made the following decisions:

(a) Member states should support development of the Regional SPS and the agricultural trade facilitation project that seeks to put into action the priority issues;

(b) Member States should support development and implementation of the Green Pass Certification Scheme;

(c) Member States should support harmonization of regulatory aspects relating to aflatoxin control including natural remedies such as bio control technologies; and

(d) Member States should support the SPS joint work programme developed by East African Community (EAC), COMESA and Southern African Development Community (SADC) for harmonization of SPS measures in the Tripartite Free Trade Area.

IMMIGRATION

Implementation of the Protocols and Council Decisions on the Movement of Persons and Labour

Decisions

16. Council made the following decisions:

(a) Member States which are yet to ratify and sign the Protocols be encouraged to do so;

(b) The chief immigration officers should play a key role in the adoption, ratification and implementation of the Protocols;

(c) The meeting of the chief immigration officers should be held more frequently in line with the rules of procedure of meetings of chiefs of immigration, which require that they meet once a year;

(d) The harmonisation of policies should take into consideration other regional obligations of Member States;

(e) The inter-linkage between the fulfilment of economic integration, economic union procedures and free movement of labour be emphasised;

(f) There is need for a paradigm shift from migration control to migration management at all institutional levels and COMESA Secretariat and cooperating partners should mobilize funding for capacity building to this effect;

(g) A task force composed of the following Member States: Burundi, Egypt, Malawi, Swaziland and Zambia and the Secretariat should work on the development of a capacity building programme that is in line with a developed road map;

(h) The implementation of the Protocols should take into consideration the several existing regional agreements to which COMESA Member States are party, in order to neutralise contradictions and promote convergence;

(i) Regional consultative processes in the form of technical workshops aimed at building the capacities of the national institutions responsible for implementation and addressing specific critical aspects should be encouraged;

(j) A specific study addressing topics, such as border and data management systems should be undertaken; and

(k) A task force composed of the following countries: Democratic Republic of Congo, Kenya, Rwanda, Sudan, Zimbabwe and the Secretariat should develop a road map for implementation of Protocols and Council decisions on the movement of persons and labour as well as harmonization of laws.

Harmonization of National Laws with COMESA Model Law

Decisions

17. Council made the following decisions:

(a) Member States which have not yet transmitted their national laws on immigration, or the draft laws to the Secretariat should do so within a three months period following the meeting;

(b) On the basis of the information submitted by Member States, and in accordance with the decision taken at the third meeting of the ministers responsible for immigration held in Lusaka, Zambia on 04 April 2008, the Secretariat should undertake a comparative study on the approximation of each Member State's national law with the model law to be considered at a workshop to be organized by COMESA and ICMPD;

(c) The line ministries, with the support of the Secretariat, should pioneer the process of reviewing their national immigration laws and take an informed decision on the need to further approximate their national legislation with the model law;

(d) The Secretariat should make the national legislation on immigration, of each COMESA Member State, available to Member States as part of a regional database; and

(e) A roadmap for the harmonisation of immigration laws should be developed by the task force established under paragraph 36(g), including a review of individual national legislation.

Cooperation on Immigration Matters among COMESA Member States to Facilitate Trade

Decisions

18. Council made the following decisions:

(a) Since the common cross border trader permits currently in use restrict rather than facilitate small cross border trade, COMESA should carry out a study on the facilitation of small, cross border trade using best practices, that will give COMESA Member States options of instruments to use to facilitate small border trade;

(b) COMESA should establish a central research and analysis unit on immigration affairs to commission, coordinate and analyse shared data across COMESA Member States;

(c) COMESA should encourage the establishment of a programme of regular direct contact among immigration officials at all levels, including staff exchange;

(d) COMESA should establish a COMESA-wide sensitization programme on the benefits of migration, promoting co-operation with, and tolerance to migrant workers;

(e) COMESA should participate in the Joint African European Union Strategy (JAES) Migration Mobility Employment (MME) partnership as a broader international cooperation framework for COMESA Member States;

(f) The Secretariat in partnership with ICMPD should organise a multi-stakeholder technical workshop to develop effective strategies to facilitate trade through increased cooperation on immigration matters.

The Africa-EU Partnership on Migration Mobility and Employment

Decision

19. Council made the following decision:

(a) That the African Union Commission (AUC) and COMESA should co-operate closely in order to ensure the effective flow of information between Member States and across the continent.

The European Union (EU) – ICMPD Migration Expertise Initiative (MIEUX)

Decision

20. Council made the following decision:

(a) That Member States should use MIEUX as a tool for capacity building and migration management.

The Joint COMESA-IOM Projects for Enhanced Cooperation

Decisions

21. Council made the following decisions:

(a) That the Secretariat, together with the International Organisation for Migration (IOM), should implement the joint initiative on institutional capacity building for Diaspora engagement and migration for development in the COMESA region; and

(b) The Secretariat should also jointly implement the initiative on capacity building and migration profiles in the COMESA region with the IOM - aimed at improving data collection and migration policy making at the national and regional Level.

Regional Approach to Border Management

Decisions

22. Council made the following decisions:

(a) There is need for the establishment of a Regional Consultative Process (RCP) for COMESA on migration management that will coordinate implementation of pilot programmes and enhance the cooperation with other institutions such as the East African Community (EAC) and Southern Africa Development Community (SADC) to harmonise their immigration instruments and policies;

(b) There is need for the development of a regional strategic plan on border management information systems that includes regional standard operating procedures on border management, using best practices from other government agencies, co-operating partners and other sub-regional organizations;

(c) There is need for the development of a harmonized curriculum for training modules; and training of immigration officials across borders, that is through utilising existing capacity available through the Africa Capacity Building Centre (ACBC) and other immigration training institutions in the region;

(d) There is need to introduce and work towards a common and linked border management information system to exchange and evaluate data. Pilot cross-

border projects on border management that involve more than one Member State that aims building capacity, combat irregular migration and establishing border management information systems; and

(e) Member States should strengthen inter-ministerial coordination on migration issues and establish cross-border immigration task forces; and report back at the subsequent meeting.

GENDER AND WOMEN AFFAIRS

7th Meeting of the COMESA Technical Committee on Gender

Decisions

23. Council made the following decisions:

(a) That Djibouti and any other Member State wishing to establish a FEMCOM chapter should contact the FEMCOM Secretariat directly for technical advice;

(b) That adequate staffing and financing of the gender programmes was necessary so that the Secretariat can effectively implement the programmes generated from the technical and ministerial meetings;

(c) That national gender machineries should lobby line ministries responsible for finance, agriculture and environment; and co-operating partners to fully implement the COMESA policy, which champions the view that 80 percent of beneficiaries of agriculture programmes should be women and female headed households; and

(d) The COMESA Secretariat should liaise with the ministries of agriculture to sensitize extension workers so that they give civic education on conservation agriculture to the rural communities because it is a low cost activity.

Establishment of the COMESA Women's Empowerment Fund

Decisions

24. Council made the following decisions:

(a) That the COMESA Women's Economic Empowerment Fund should be established by the next Council and Summit;

(b) That upon the establishment of the Fund, the manager should develop an operational manual that would contain the following principles:

i) An organogram be developed in order to illustrate the relationship between different levels of management and the Fund structures.

ii) The size of the Fund should be determined after the feasibility study and the COMESA Secretariat should organise a forum of women entrepreneurs at country level to collect information and recommendations on the size of the fund.

iii) The apex level of the Fund should establish mechanisms for collaboration with co-operating partners and NGOs for implementation of the Fund in a transparent manner.

iv) The apex level, in collaboration with the intermediary financial institutions, should establish reasonable tenure, interest rates, and grace period to create an enabling environment for women to benefit from the Fund.

v) National gender machineries, in collaboration with the COMESA Secretariat, should intensify civic education to demystify the cultural perceptions that discredit women entrepreneurs.

vi) Efforts be made to ensure equality in treatment of all beneficiaries without regard to the type of business that they do, and socio-status.

vii) Member countries in collaboration with COMESA Secretariat should compile directories or compendium and conduct a social audit of what is available.

viii) The Fund Manager should propose a monitoring and evaluation mechanism to ensure equity in terms of Member States benefiting from the Fund.

ix) The apex level, in conjunction with the Fund Manager, should negotiate with partner financial intermediaries on issues regarding the interest rates to be charged and other fees; and

x) Negotiate favourable interest rates with the intermediary financial institutions.

The COMESA Trading House Project

Decisions

25. Council made the following decisions:

(a) Member States should implement the Trading House Project by 2014;

(b) The Secretariat should undertake appraisal of the functionality of the trading houses in Member States;

(c) Member States who are ready to establish trading houses could proceed with the activity;

(d) Policy formulation should take place simultaneously with the establishment of a trading house;

(e) The project should involve other partners such as the International Labour Organisations, (ILO) ministries of finance, and Non Governmental Organisations (NGOs) as implementing partners; and

(f) The COMESA Secretariat should engage the Government of Japan and other partners through their embassies and share their experiences on how trading houses operate in Japan with a view to securing their support and where possible to arrange a study visit for the ministers to trading houses in Japan.

Engendering Climate Change in the COMESA region

Decisions

26. Council made the following decisions:

(a) The COMESA Secretariat, in collaboration with Member States, should conduct sensitization programmes for women on climate change since more women are working in agriculture;

(b) The COMESA Secretariat, in collaboration with Member States, should review and analyse the policies and regulations and the National Adaptation Programmes of Action (NAPAs) from a gender perspective;

(c) The COMESA Secretariat and Member States should include women in the design and implementation of the agriculture and climate change programmes;

(d) Noted the executive brief on the regional strategy on gender mainstreaming in agriculture and climate change; and requested the Secretariat to circulate the finalised document by the second week of October 2011.

The Human Immunodeficiency Virus/Acquired Immune Deficiency Syndrome (HIV/AIDS) Multi-Sectoral Programme

Decisions

27. Council made the following decisions:

(a) The COMESA Secretariat should mobilise resources in order to implement the strategies and provide progress reports on the implementation of the HIV and AIDS programme to Member States.

(b) The committee noted the HIV and AIDS regional programme and requested the Secretariat to circulate the finalized document by the second week of October 2011.

COMESA Gender Mainstreaming Manuals

Decision

28. Council made the following decision:

(a) Adopted the COMESA gender mainstreaming guidelines/manuals and directed the Secretariat to distribute them to Member States.

MINISTERS OF JUSTICE AND ATTORNEYS GENERAL

Charter of the COMESA Regional Investment Agency

Decision

29. Council made the following decision:

(a) Approved the draft revised charter attached as Legal Notice 16(1).

Assessment of the Permanent Court Facilities of the COMESA Court of Justice

Decisions

30. Council made the following decisions:

(a) Adopted the report of the sub-committee of the COMESA Ministers of Justice and Attorneys General on the assessment of permanent facilities for the COMESA Court of Justice in Khartoum.

(b) Urged the Government of Sudan to work with the Court and the Secretariat to finalise outstanding issues on the court for a hand over to the court.

(c) Decided that the Court building should include a surveillance system to enhance the security of the court.

COMESA COURT OF JUSTICE

Decisions

31. Council made the following decisions:

(a) That Member States should continue to pay their assessed contribution timely, in accordance with Articles 42(4) and 166(6) of the COMESA Treaty.

Court Publicity Seminars

Decisions

32. Council made the following decisions:

(a) The Court should, as soon as is feasible, redouble its efforts to publicize itself and sensitize its users in all Member States;

(b) Seminars should be organized in conjunction with national Judiciaries, law societies, chambers of commerce and similar court users; and

(c) In order to achieve the required results, more funding should be provided to the budget of the Court.

Status of Contributions to the Court

Decisions

33. Council made the following decisions:

(a) Mauritius, which has paid up her 2011 contributions, be commended;

(b) Egypt, which has cleared her arrears and paid up her 2011 contribution, be commended and urged to clear her interest on arrears;

(c) Kenya, which has paid 50 percent of her 2011 contribution, be commended and reminded to pay her remaining balance;

(d) Burundi, Democratic Republic of Congo, Djibouti, Eritrea, Libya, Rwanda, Seychelles, Swaziland and Zambia who have paid their contributions up to 2010, be commended and urged to pay their 2011 assessed contributions;

(e) Ethiopia, Malawi and Zimbabwe, who paid their contributions up to 2009, be urged to pay their balances and their 2011 assessed contributions;

(f) Union of Comoros, Sudan, Uganda and Madagascar have arrears of more than two years and should be encouraged to enter into repayment plans that will ensure payment of arrears and interest thereon in instalments while remaining up to date with current assessment.

(g) That Member States should as much as possible comply with Treaty provisions in terms of being up to date with their obligations in relation to contributions to the COMESA Court of Justice.

INFRASTRUCTURE
Policy Harmonisation

Transport and Communications Strategy and Policy (TCS)

Decisions

34. Council made the following decisions:

(a) The Secretariat should, through the Tripartite Task Force, harmonize the policies and strategies at Tripartite level;

(b) Member States should appoint focal points in the relevant ministries to coordinate implementation of COMESA programmes and liaise with the Secretariat and submit the names of the focal points to the Secretariat by December 2011;

(c) Member States should establish or revive the multi-disciplinary, national technical working groups;

(d) The Secretariat should work with Member States and assist them to domesticate the policy and strategy into national legislation; and

(e) The Secretariat should publish the Model Transport and Communications Policy and Strategy to be used as reference documents and circulate it to Member States by December 2011.

Policy on Cyber Security

Decisions

35. Council made the following decisions:

(a) The Model Cyber Security Policy, Model Bill, Cyber Security Implementation Roadmap respectively be adopted; and

(b) The COMESA Secretariat as the Chairperson of the Tripartite Task Force (TTF) to undertake the harmonization of the cyber security policies within the tripartite framework.

Broadcasting Sector Reform Programme

Decisions

36. Council made the following decisions:

(a) The Secretariat should integrate the work carried out by the EAC and SADC in the study on the broadcasting sector reform to be undertaken in order to ensure that the outcomes and recommendations of the study take into account the decisions already undertaken and activities being already implemented by some Member States;

(b) Member States should participate in the workshop and provide the necessary information required for the study; and

(c) The Secretariat should develop and organize a capacity building programme for regulators and policy makers on broadcasting sector reform.

E-learning strategy

Decision

37. Council made the following decision:

(a) Adopted the e-Learning Strategy**.**

E-transaction Model Law

Decision

38. Council made the following decision:

(a) That the Electronic Transaction Model Bill contained in Volume 16 (2) of this gazette be adopted.

E-Waste

Decisions

39. Council made the following decisions:

(a) The Secretariat should conduct a study to draw up a regional model policy on e-waste by March 2012;

(b) The Secretariat should sign the Memorandum of Understanding with the Solving the E-waste Problem (StEP) initiative; and

(c) The Secretariat should develop a regional e-waste management system.

E-Learning Programme

Decision

40. Council made the following decision:

(a) That Member States that have not yet provided details of their e-learning focal points to the Secretariat be urged to do so by end of October 2011.

The COMESA Model Energy Policy Framework

Decision

41. Council made the following decisions:

(a) That the COMESA Secretariat as the Chairperson of the Tripartite Task Force (TTF) should undertake the harmonization of the energy policies within the Tripartite framework.

Liberalisation of Air Transport

Decision

42. Council made the following decisions:

(a) That Member States be urged to grant fifth freedom and other traffic rights to other Member States in accordance with the provisions of the Legal Notice No. 2 of 1999 and the Yamoussoukro Decision**.**

Competition Regulations for the Liberalization of Air Transport Services within COMESA, EAC and SADC

Decision

43. **Council made the following decisions:**

(a) That Member States be urged to facilitate the work of the consultants to provide the necessary data for the study on competition regulations for the liberalisation of air transport services within the region.

The COMESA Cooperative Development of Operational Safety and Continuing Airworthiness Programme (COSCAP) Project

Decisions

44. Council made the following decisions:

(a) That Member States be urged to fund the COSCAP project through the civil aviation authorities; and

(b) The Secretariat should prepares COMESA-COSCAP project with modalities for funding by Member States taking into account the SADC and EAC projects and submit it through the civil aviation authorities for approval by Member States.

Road Transport

Decisions:

45. Council made the following decisions:

(a) On trade and transit transport facilitation; Council decided that Member States be urged to participate actively in the development of multi-lateral trade and transport facilitation instruments being developed for the entire Eastern and Southern African (ESA) region.

(b) On vehicle overload control; Council decided that once adopted by the EAC Policy Organs, the agreed regional framework should be complied with by all Member States; all Member States should implement the regional axle load limits; and the Tripartite Task Force should expedite the drafting of an ESA wide legislation on axle load limits and vehicle over load control.

(c) On management and funding of maintenance of road infrastructure; Council decided that:

i) Member States be urged to strengthen and ensure sustainability of road funds and agencies and to share good practices through capacity building and information sharing; and

ii) The Secretariat should establish an association of road agencies to facilitate harmonisation and capacity building.

Railways Operation and Management

Decisions

46. Council made the following decisions:

(a) The Secretariat should develop capacity building programmes for railways engineers and other related professionals, including expert exchange programmes among Member States; and

(b) Member States be urged to take an active part in the preparation of the model railway services agreement, regulatory framework and management systems to enhance railway efficiency in the COMESA region.

Corridor Development and Management

Decisions

47. Council made the following decisions:

(a) Corridor Coordinating Committees (CCC) should be established for the following corridors to facilitate coordination, joint programming and resource mobilisation for corridor developments in the region:

i) Central Corridor – Tanzania, Rwanda, Burundi and DR Congo.
ii) Djibouti Corridor – Djibouti, Ethiopia, Sudan and South Sudan.
iii) Lamu Corridor – Kenya, Ethiopia, Sudan and South Sudan.
iv) Northern Corridor – Kenya, Uganda, Rwanda, Burundi, DR Congo and South Sudan.

(b) The Secretariat should facilitate the operationalisation as well as the activities of the CCCs.

Maritime Security

Decisions

48. Council made the following decisions:

(a) Member States, through the maritime regulatory authorities, should facilitate negotiations among shipping lines, shippers and ports; and

(b) Port authorities and Member States are urged to participate in the Swakopmund, Namibia PMAESA Conference in December 2011.

Egyptian Government Capacity Building Programme

Decision

49. Council made the following decision:

(a) Urged Member States that had committed to taking up scholarships for the Masters in Science degree programme at the Arab Maritime Academy in Alexandria to nominate candidates for the programme.

Inland Water Transport

Decisions

50. Council made the following decisions:

(a) The Secretariat should assist Member States to adapt and customise standards and regulations based on the already developed international standards by the IMO.

(b) Member States be encouraged to join IMO;

(c) The Secretariat, under the Tripartite framework, should develop institutional framework and mechanisms to build capacity for search and rescue for the inland waterways; and

(d) Multilateral agreements be entered into by countries sharing common water bodies in order to enhance harmonized management of the resources in such water bodies.

Information and Communications Technologies (ICT)

ICT Mainstreaming

Decisions

51. Council made the following decisions:

(a) The Secretariat should develop guidelines for mainstreaming ICT into infrastructure programmes; and

(b) Member States should mainstream ICT in their infrastructure programmes

Information Society Measurements

Decisions

52. Council made the following decisions:

(a) Member States should establish information centres for ICT data if they have not done so;

(b) Multi-purpose surveys carried out by bureau of statistics offices should include ICT sector data; and

(c) Member States are requested to produce annual or biannual ICT bulletins.

ICT Consumer Protection Project

Decisions

53. Council made the following decisions:

(a) Member States be urged to implement the COMESA Consumer Protection policy guidelines;

(b) The Secretariat should support consumer protection associations;

(c) Regulators be urged to reduce mobile termination rates and facilitate mobile network coverage; and

(d) Regulators should implement number portability.

Newly Established Postal Regulators

Decisions

54. Council made the following decisions:

(a) Member States should participate in the post code and addresses system project and provide all the necessary information;

(b) The Secretariat should organize a programme for capacity building on post code and addresses;

(c) Postal regulators be requested to participate in the training; and

(d) Postal regulators be requested to provide their inputs for the 25th United Postal Union (UPU) Congress.

Association of Regulators of Information and Communications Service of Eastern and Southern Africa (**ARICEA)**

Decisions

55. Council made the following decisions:

(a) Countries should submit their comments on the ARICEA draft host agreement by 30 Sept 2011;

(b) The host agreement be revised by COMESA by October 2011;

(c) The Secretariat should present the revised agreement to Executive Committee in February 2012; and

(d) The Secretariat should present the host agreement to the COMESA Policy Organs.

Next Generation Network (NGN)

Decisions

56. Council made the following decisions:

(a) The Secretariat should develop a concept paper on the study on the readiness of Member States to migrate and deploy Next Generation Network and broadband connectivity;

(b) The study should develop a road map for the implementation of NGN and broadband connectivity;

(c) The study should also come out with enabling policy and regulations to pave way for migration and deployment of NGN and broadband connectivity; and

(d) The COMESA Secretariat should conduct the study in collaboration with International Telecommunications Union (ITU).

Infrastructure Sharing

Decision

57. Council made the following decision:

(a) That the Secretariat should develop policy guidelines on infrastructure sharing**.**

Standards and Type Approval Capacity Building

Decision

58. Council made the following decisions:

(a) That the Secretariat should convene a workshop on ICT standardisation for all Member States.

Remittance of ARICEA contributions

Decisions

59. Council made the following decisions:

(a) That Member States with arrears should pay their contribution; and
(b) All members should include the ARICEA contributions in their budget.

INFORMATION TECHNOLOGY (IT)

Decisions

60. Council made the following decisions:

(a) The Secretariat should proceed with the development of the two systems (the cross-border trader's information system and an online business directory); and

(b) Member States should provide the required data for the regional information systems once they become operational.

Geographical Information Systems (GIS)

Decisions

61. Council made the following decisions:

(a) The Secretariat should publicise the GIS; and

(b) More layers such as peace and security and statistics be added to the GIS.

ICT Trade Facilitation

Decisions

62. Council made the following decisions:

(a) The Secretariat should set up the ICT trade facilitation support centre;

(b) The Secretariat should share with the countries their ICT trade facilitation projects;

(c) The Secretariat should continue its support on ICT Trade Facilitation tools and projects for the Member States; and

(d) Member States using ASYCUDA++ be urged to migrate to ASYCUDA WORLD.

Sustainability of Information Systems

Decisions

63. Council made the following decisions:

(a) That Member States should adopt the guidelines that were prepared for them to ensure sustainable update of content; and

(b) The Secretariat should recruit a web marketing consultant.

Free and Open Source Software (FOSS)

Decision

64. Council made the following decision:

(a) That the Secretariat should ensure that the FOSS workshop is held and Member States are requested to develop policy guidelines on FOSS.

E-Government Programme

Decisions

65. Council made the following decisions:

(a) The COMESA Secretariat, together with the Government of Uganda, should fast track the signing of the Memorandum of Understanding providing for the establishment of the regional e-Governance academy; and

(b) Member States that have not submitted the details of the e-Government focal points are requested to do so as soon as possible.

The COMESA Strategic Meteorological Programme

Decision

66. Council made the following decision:

(a) That the Secretariat should convene a meeting of the meteorological authorities to update the status of implementation of the Comprehensive Meteorological Programme adopted by Council and agree on a framework for co-operation in the implementation of the programme.

The Regional Association of Energy Regulators for Eastern and Southern Africa (RAERESA)

Decision

67. Council made the following decision:

(a) That the members of RAERESA be requested to contribute to the budget of running the Secretariat of RAERESA.

Renewable Energy

Decision

68. Council made the following decision:

(a) That Member States should provide information on renewable energy in order to assist in the preparation of a COMESA programme for development of renewable energy.

The Communications Navigation Surveillance/Air Traffic Management (CNS/ATM) Systems Project

Decisions

69. Council made the following decisions:

(a) Member States in the CNS/ATM Working Group (WG) should appoint/nominate their representatives by end of October 2011;

(b) The Secretariat should convene a meeting of the Tripartite Civil Aviation;

(c) Authorities should establish an institutional framework for implementing the Tripartite CNS/ATM systems programme;

(d) Rwanda as chair of the CNS/ATM WG be commended for the leadership and resources provided for the project; and

(e) AfDB be commended for the grant extended to COMESA for the CNS/ATM systems project.

The Shire-Zambezi Waterways Project

Decisions

70. **Council made the following decisions:**

(a) That the parties to the MoU on the implementation of the Shire-Zambezi waterways project:

i) Be urged to participate in the Joint Tripartite Committee (JTC) meeting and agree on the their requirements for the conditions precedent to the first disbursement of the grant;

ii) Be urged to expedite fulfilment of the conditions precedent so that the projected implementation can be started without any undue delays;

iii) Be urged to support the work of the consultants as they conduct the feasibility studies and the environmental impact assessments in their territories;

iv) Rehabilitate of the Lukuga Barrage.

Great Lakes Railways Project

Decision

71. Council made the following decision:

(a) That the participating Member States be urged to provide information for the study and to participate in the validation events of the pre-feasibility study on the Great Lakes Railway network.

The COMTEL Project

Decisions

72. Council made the following decisions:

(a) The Secretariat should float an international tender for the private sector to prepare a proposal for a Private Public Partnership (PPP) arrangement for implementing the COMTEL project with willing

National Telecommunications Operators (NTOs) and other service providers;

(b) The Secretariat should develop a mechanism for joint utilization and interfacing of the existing facilities at the border points in order to create seamless communication across the border with a view to reducing the tariff costs; and

(c) Member States be urged to harmonise policies and tariff regimes**.**

Very-Small-Aperture Terminal (VSAT) Closed User Group Communications Network

Decisions

73. Council made the following decisions:

(a) Malawi, Seychelles and EAC be requested to change their private automatic branch exchange (PABX) to suit the VSAT system as agreed before 15 October 2011;

(b) Member States relocate the telephone lines to COMESA coordinators and PS offices if they had not done so; and

(c) Financial resources be allocated to maintain the project and activate other services such as video conferencing.

The Northern Corridor VSAT Network

Decision

74. Council made the following decision:

(a) That Member States covered by the project facilitate the work of the contractor in order have a smooth implementation of the project within the contractual period.

The Eritrea/Sudan and Uganda/Sudan Power Interconnection Projects

Decision

75. Council made the following decision:

(a) That Eritrea and Uganda be urged to endorse the Project Information Memorandum (PIM), the Inter-Government Memorandum of Understanding (MOU) and Inter-Utility MoU in order to fast track the implementation of the two projects.

Co-operation with other Regional Economic Communities

Decisions

76. Council made the following decisions:

(a) That Member States served by the four corridors be urged to participate in the Tripartite and the IGAD Infrastructure Investment Conference; and

(b) Donors, development partners and the private sector be called upon to support the conference and to give financial support to the infrastructure programmes and projects along the four major regional corridors in the ESA region.

Programme for Infrastructure Development in Africa (PIDA)

Decisions

77. Council made the following decisions:

(a) A mechanism should be established to facilitate implementation of the projects that have already been identified by Member States that have an impact on regional integration; and

(b) Member States be requested to actively participate in the PIDA workshop to be held in Nairobi, Kenya from 30 September to 01 October 2011.

INTERGOVERNMENTAL COMMITTEES

Standardization and Quality Assurance Committee (SQA)

Decisions

78. Council made the following decisions:

(a) On standards harmonisation it was decided that:

i) A strategic plan to guide the implementation of the SQA policy should be developed taking into account the common challenges facing Member States in quality infrastructure and to meet the requirements of the Customs Union;

ii) The mechanism for the development and implementation of COMESA standards should be aligned with the SQA activities; and

iii) The 65 electrical standards be adopted.

(b) On the metrology and legal metrology it was decided that:

i) Member States and the Secretariat should avail resources for the implementation of the identified activities to enable recognition of metrology services regionally and internationally; and

ii) There should be full participation of COMESA at the Intra-Africa Metrology System as a sub-regional metrology organization.

(c) On accreditation it was decided that:

i) Member States be urged to liaise for the purpose of recognizing each other's accreditation activities.

(d) On technical regulations it was decided that:

i) The Secretariat should expedite the operationalisation of a sub-committee on technical regulations.

(e) On testing and quality assurance it was decided that:

i) Member States be urged to liaise with each other for the purpose of recognition of each other's test reports and certificates while a scheme of mutual recognition is being developed.

(f) On mutual recognition of accreditation and reduction of trade barriers, it was decided that:

i) Detailed, technical regulations should be developed for mutual recognition of technical standards, with a view to eventually establish a COMESA regional accreditation centre.

ii) There is need for standardisation of road infrastructure in order to promote interconnectivity in the COMESA region

Trade and Customs Committee

Decisions

Council made the following decisions:

79. On Trade Developments:

(a) Programmes to increase intra-COMESA trade should be up-scaled, through interventions such as annual trade fairs, promotion of value addition and regional value chains, and building of soft and hard infrastructure, and removal of Non Tariff Barriers (NTBs);

(b) The Secretariat should continue work on preference utilisation, in order to better disaggregate trade data;

(c) Work on trade flow analysis, including a comprehensive data base on both industrial and agricultural products and value

chains in order to provide better information to stakeholders, should be advanced;

(d) Better publicity of trade fairs in the region should be undertaken by Member States and the Secretariat;

(e) There is need for COMESA promotion activities at the international and regional levels with a COMESA seal or a regional dimension; the trade fairs should rotate from country to country organised jointly with the Secretariat;

(f) Member States are urged to provide relevant data on a timely basis to assist data compilation and analysis;

(g) To address the low share of manufacturers in intra-regional trade, programmes for value addition and industrial development to increase the share of manufacturers in COMESA intra-regional trade should be up-scaled, building on on-going programmes such as those for increasing productivity and market analysis and information; and

(h) In addition to trade performance, reports on the internal markets should be including intra-COMESA cross-border investment flows as well as data on the level of trade in manufactured products.

80. On participation in the Free Trade Area (FTA)

(a) There is need for a matrix showing the status on the extent of tariff reduction undertaken so far by the Member States that are not yet in the FTA;

(b) The Member States should provide a time table for joining the FTA, unless they will be completing the elimination of customs duties in one step;

(c) All the Member States should participate in the COMESA FTA and in this regard should speedily finalise their internal processes for joining the FTA; and

(d) The DR Congo is commended for the decision to join the FTA and participate in the internal market.

81. On Non-Tariff Barriers (NTBs)

(a) The programme for mutual recognition of technical standards and SPS measures should be enhanced and harmonisation should be expedited;

(b) Information should be provided on standards so far harmonised, with a focus on products that are traded in the region;

(c) The Secretariat should liaise with Madagascar to ensure that the Council Decision is implemented and will keep Mauritius informed; and

(d) The Secretariat should facilitate the study tour on milk and milk products as agreed between Kenya and Zambia at the last meeting of the Trade and Customs Committee.

82. On draft NTB Regulations

(a) A meeting of the working group on NTB Regulations should be convened in the last quarter of the year to address all outstanding issues and finalise the draft regulations for consideration by the next Policy Organs' meetings.

83. On Rules of Origin

(a) Adopted the Change in Tariff Heading (CTH) Rules for the chapters that were outstanding, as contained in Annex I, and decided as follows:

i) The Secretariat should undertake capacity building and training based on needs assessment and on a case by case basis for stakeholders, especially customs officers;

(a) The Secretariat should conduct a new study on the impact of rules of origin on intra-COMESA trade; the study should

cover rules of origin for the Tripartite FTA as well as COMESA's capacity in the production of edible oils derived from among others: corn, soya beans, sunflower, ground nuts, cotton seed, and palm seed. The study should also cover raw materials and manufacturing capacity taking into account actual and pledged investments into the sector, revenues, consumption, employment and other relevant parameters;

(b) Appropriate flexibility will be necessary for the CTH rules on edible oils (Chapter 15), where the raw materials are not available in the region; and

(c) A meeting of the Working Group on Rules of Origin should be convened to consider and implement these Decisions.

Review of implementation of the Transition Period for the Customs Union

Lists of Sensitive Products

Decisions

84. **Council made the following decisions**:

(a) The lists of sensitive products submitted by Member States will remain provisional and should be attached as annexes to the Council Regulations governing the Customs Union with a clear note indicating that they are provisional in nature and will be replaced by the final lists once finalized. The submitted lists of sensitive products are attached as Annexes II to VI;

(b) Implementation of the transition period, with respect to the Customs Management Regulations and the Common Tariff Nomenclature, should proceed in accordance with the Council Decisions;

(c) Member States should finalise their tariff alignment schedules to the CET, and pending which the drafts produced by the Secretariat should be considered for annexing to the Council Regulations on a provisional basis, and will be replaced by the final schedules once finalized; and

(d) Burundi, Rwanda, and Uganda, as partner states in a Customs Union, consider using a common list of sensitive products, namely, the version submitted by Kenya.

Common External Tariff (CET)

Decisions

85. **Council made the following decisions**:

(a) The Secretariat should work more closely with the Member States that need assistance in the implementation of the transition period for the Customs Union;

(b) COMESA should continue to implement Council Decisions on the Customs Union together with the Tripartite FTA;

(c) A study should be conducted on the interface between the Tripartite FTA and the Customs Union and the implications of the Customs Union on the Tripartite process; and

(d) The study on countries with a substantial number of tariff lines below the CET rates should also be revised, and Egypt and Zimbabwe will be included in the revised study, and the revised study will consider the impact on competitiveness and industrialisation. The outcome of the study should determine the tariff alignment schedules for Member States with a substantial number of tariff lines with rates below the CET.

The Services Liberalisation Programme

Decisions

86. **Council made the following decisions**:

(a) The draft schedules of specific commitments in the four priority sectors considered by the Third Meeting of the Committee on Trade in Services, as improved, should be used in the negotiations for the services liberalisation programme;

(b) Member States are at liberty to undertake commitments in any other priority sectors they indicated and are urged to work closely with the Secretariat in finalising their improved draft schedules in these other sectors;

(c) The Committee on Trade in Services should make good progress in taking forward the services liberalisation programme;

(d) The World Bank be commended on the partnership on the Knowledge Platform as a data base that will provide useful information for taking forward the services liberalisation programme, and on facilitating stakeholder workshops on professional services;

(e) The Secretariat will provide technical assistance to Member States that need such assistance; and

(f) Member States that haven't submitted their revised and final drafts of schedules of specific commitments should do so by 30 October 2011.

Multilateral Trade Negotiations

Decision

87. **Council made the following decisions**:

(a) COMESA should take a position as early as possible on certain key issues, especially the Least Developed Country (LDC) package, taking into account that extension of Africa Growth and Opportunity Act (AGOA) preferences by the US Government to other LDCs will have an adverse impact on African AGOA eligible countries;

(b) The Secretariat should prepare a technical paper on key issues with proposals for positions, and circulate to Member States for consideration before the World Trade Organisation (WTO) Ministerial Conference;

(c) The positions should be advanced also within the frameworks of the Africa Group, the ACP Group, the LDC Group, and the G90 Group; and

(d) COMESA should effectively prepare for the Eighth Ministerial Conference, including through national and regional processes as well as within the framework of the coalitions.

Africa Growth and Opportunity Act (AGOA)

Decisions

88. **Council made the following decisions**:

(a) The Government of Zambia be commended for successfully hosting the Tenth AGOA Forum and other Member States for their active participation, including in terms of preparing a common position to advance while engaging the US Government;

(b) AGOA should be extended beyond 2015 and the third country fabric provision be extended beyond 2012, and in this regard, the extensions should take into account the need for predictability to assist better planning and to promote investment, which require a reasonably long period; and

(c) The US State Department be commended for indicating willingness to extend the duration of AGOA and the third country fabric provision. The meeting requested the Secretariat to continue engaging the various stakeholders for

example the White House and Congress that can assist to advance the initiative of extending AGOA and the third country fabric provision.

The Regional Customs Transit Bond Guarantee Scheme (RCTG)

Decisions

89. Council made the following decisions:

(a) Commended the close collaboration between COMESA and EAC in implementing the RCTG Scheme, and encouraged the Secretariat to continue involving Tanzania and Mozambique in the programme.

(b) A joint meeting between Djibouti and Ethiopia together with the Secretariat should take place to advance the implementation of the RCTG Scheme on the Djibouti-Addis Corridor.

Intellectual Property (IP)

Decisions

90. Council made the following decisions:

(a) Adopted the COMESA Policy on Intellectual Property Rights and Cultural Products;

(b) Member States, with assistance from the Secretariat and cooperating partners, should undertake an audit of all relevant IP and related laws, policies, and institutions, as well as their IP assets;

(c) Member States should promote investment in Research and Development in order to develop IP assets;

(d) In implementing the COMESA IP Policy, emphasis should be put on the development priorities of the region, such as geographical indications, access to medicine, cultural products, traditional knowledge, bio-piracy and follow up on infringement of regional IP assets;

(e) Adopted the COMESA Strategy for the Pharmaceutical Sector;

(f) Adopted the guidelines for preparing national intellectual property policies; and

(g) Called upon Member States to make good progress in implementing the other priorities of the intellectual property programme such as undertaking audits of IP assets, protecting and promoting geographical indications, protecting and promoting traditional medicine, taking measures against bio-piracy, and following up on infringement of regional IP assets.

Single Window

Decision

91. **Council made the following decision:**

(a) Endorsed the Single Window Programme and called for its operationalisation.

Science Technology and Innovation

Decision

92. Council made the following decision:

(a) Adopted the Strategy and Implementation Plan, attached as Annex 15; and

(b) Directed that the Second Meeting of the Science, Technology and Innovation Committee should be held in the last quarter of the year, and among other things the meeting

should identify regional science and technology parks, and regional clusters.

Statistical Matters

Decisions

93. Council made the following decisions:

(a) The Secretariat and Member States should develop a programme on trade in services statistics based on the recommendations of the joint COMESA-Commonwealth Secretariat workshop;

(b) The Secretariat and Member States should develop country specific roadmaps on the development of trade in services statistics;

(c) Member States' statistical offices should set up infrastructure statistics units in order to entrench the coordination, compilation and dissemination of infrastructure statistics in the national statistical system;

(d) Member States should improve the scope and quality of macro-economic data; and

(e) The national accounts interventions be realigned to focus on targeted studies on issues, which posed implementation challenges in the SNA 1993.

CROSS CUTTING ISSUES

Aid for Trade

Decision

94. Council made the following decision:

(a) That the COMESA Aid for Trade Strategy should be revised through a consultative process and should cover a four year period (2012-2015) aligned to the Mid Term Strategic Plan (MTSP).

Institutional Development

Decision

95. Council made the following decision:

(a) That a COMESA Conference of Ministers of Industry should be organised, taking into account the on-going work of the African Union Conference of Ministers of Industry.

The COMESA-EAC-SADC Tripartite Arrangement

Decisions

96. Council made the following decisions:

(a) Member States should immediately submit current, national tariffs and all trade measures to the Secretariat and regularly update the Secretariat on any subsequent changes implemented at national, regional or multilateral levels for circulation to other REC countries as part of the Tripartite transparency mechanism envisaged under the preparatory phase;

(b) Member States should validate the information and data circulated by the Tripartite Task Force;

(c) Member States should commence, or intensify, national consultations and preparation of national negotiating positions for core Tripartite FTA issues and the movement of business persons negotiations;

(d) COMESA should regularly hold meetings on the Tripartite to consider the implementation of the outcome of the Second Tripartite Summit and to prepare for the Tripartite Free Trade Area Negotiations, beginning in the last quarter of 2011; and

(e) The paper on the implementation of Tripartite FTA be circulated to Member States for their consultations; and

(f) The Secretariat should examine the possibility of holding a pre-Tripartite meeting before the aforesaid meeting of the Tripartite Task Force.

Reports by Member States on COMESA Programmes

Decisions

97. Council made the following decisions:

(a) Member States that have produced written reports should transmit them to the Secretariat, which should circulate them to all Member States; and

(b) Member States that have not prepared written reports using the new format should endeavour to finalise their reports and transmit them to the Secretariat for circulation. Member States that wish to be assisted in this regard should contact the Secretariat.

Reports of COMESA Institutions

The Eastern and Southern Trade Development (PTA) Bank

Decisions

98. Council made the following decisions:

(a) Urged those Members of COMESA who have not yet joined the Bank to do so; and

(b) Urged Members States who have not fully settled their obligations under the Bank's General Capital Increase Programme to do so in order to strengthen the Bank's capital base and enhance its status in the international market.

RE – Insurance Company (ZEP-RE)

Decisions

99. Council made the following decisions:

(a) On the hosting of the company, the Republic of Zimbabwe was urged to conclude the approval process and allow ZEP-RE to set up an office in Harare as soon as possible, to enable the Company to underwrite business directly from the market.

(b) On business facilitation, Malawi was urged to formally recognise ZEP-RE as a local reinsurer and allow the institution to directly underwrite business from local insurers in line with the Member States' internal regulations.

(c) Swaziland and Libya were urged to facilitate business cessions from their respective territories in line with commitments made in the past.

(d) On capital subscriptions, in line with the undertaking made by the Member States during the 14th Council of Ministers meeting in 2002, Ethiopia was urged to subscribe for shares in ZEP-RE.

(e) Malawi, Libya, Swaziland and Uganda were also urged to consider purchasing shares in ZEP-RE.

African Trade Insurance Agency (ATI)

Decisions

100. Council made the following decisions:

(a) Gratitude be conveyed to the World Bank for its continued technical and financial support for ATI's membership expansion; and

(b) African countries, especially COMESA Member States, which are not yet ATI members consider joining the Agency and by doing so bring the benefits of ATI's products to investors and the business communities in their respective countries.

Federation of National Associations of Women in Business in Eastern and Southern Africa (FEMCOM)

Decisions

101. Council made the following decisions:

(a) Increase resources for effective and efficient operations of the FEMCOM Secretariat and activities; and

(b) COMESA should consider increasing funding for hiring of professional staff at FEMCOM Secretariat.

Competition Commission

Decision

102. Council made the following decisions:

(a) That Member States without national competition legislation should enact competition laws in line with COMESA regulations.

Alliance for Commodity Trade in Eastern and Southern Africa (ACTESA)

Decisions

103. Council made the following decisions:

(a) Urged ACTESA to cover all Member States when implementing its programmes;

(b) Adopted the ACTESA Five-Year Development Strategy (2012-2016);

(c) Directed ACTESA to develop an action plan for the implementation of the strategy;

(d) Directed ACTESA to develop a Charter to govern the operations of the agency; and

(e) Directed ACTESA to develop a monitoring and evaluation mechanism to track performance and assess the effectiveness of the strategy.

Regional Integration Support Mechanism (RISM) Indicators

Decisions

104. Council made the following decisions:

(a) Approved the Integration Indicators that are in line with the MTSP, as set out in the table below;

(b) Urged Member States to finalise their baselines against the MTSP monitoring system;

(c) Urged Member States to constitute, formalise and notify the Secretariat of their national inter-ministerial co-ordinating committees; and

(d) A workshop on preparation of requests under next call for submissions be held before the end of 2011.

Table: Integration Indicators

PRIORITY AREA 1: REMOVING BARRIERS TO FACTOR MOBILITY		
Intervention Area	**Outcome**	**Indicator**
National Inter-Ministerial Coordinating Committees set up	Framework for drafting, monitoring and reporting on implementation of commitments	RISM national focal points nominated
		National monitoring committees constituted and meeting regularly
Consolidate the internal market (Free Trade Area)	Eritrea, Ethiopia, RD Congo and Uganda join FTA by 2012	Eritrea, Ethiopia, RD Congo and Uganda join FTA
	Steps and Measures to eliminate barriers to trade (Standards, SPS and NTBs) agreed on by 2012	NTBs online monitoring system functioning and NTBs reported by the private sector
		Institutional structures such as national focal points and national monitoring committees on NTBs established by all Member States by 2012
		Member States gazette the NTB Regulations
		Regional SPS (Sanitary/Phyto-sanitary) measures adopted and implemented
		Number of Standards being implemented by MS
		Countries implementing mutual recognition certificates for Standards and SPS
Operationalise the Customs Union	All countries domesticate the Common Tariff Nomenclature (CTN) by 2012	CTN domesticated
	14 countries implementing 80% of the Common External Tariff (CET) by 2015	% of the CET implemented by MS
	Regional sensitive products list agreed by 2012	Sensitive products list submitted by MS
	14 countries domesticate the Customs Management Regulations (CMR) by 2012	Customs Management Regulations domesticated
	Member states implementing the CMR Guidelines	Member states implementing the CMR Guidelines
	Implementation of the Customs Union Road Map for the transition period	Member States submit and implement Schedule I, II and III of Tariff Alignment schedule

Launch of the Common Market by 2015	Implement Council Regulations on Free Movement of goods, Services, Labour, Persons and Capital and Recognition of Right of Residence and Establishment	Member States sign and ratify the Protocol
Trade in Services	Finalized schedule of commitments in the priority sectors presented by MS	Member States submit schedule of commitments
	Regulations on trade in services implemented	Member States domesticate regulations on trade in services
Common Competition Policy	Member States adopt the enforcement guidelines and procedures of the Competition Regulations	Enforcement guidelines and procedures of the Competition Regulations adopted by Member States
COMESA Regional Policy on Intellectual Property rights and Cultural Industries	COMESA Regional Policy on intellectual property rights and culture implemented	Acts ratified and gazette into national law
PRIORITY AREA 2: BUILDING PRODUCTIVE CAPACITIES FOR GLOBAL COMPETITITVENESS		
Foreign Direct Investment and Domestic Investments	MS sign and ratify the investment agreement of COMESA Common Investment Area (CCIA)	MS sign and ratify the investment agreement of COMESA Common Investment Area (CCIA)
	MS to domesticate the CCIA into national law	CCIA domesticated by Member States
	MS submitting the sensitive temporary exclusion list of the economic sector with regard to the liberalization programme	MS submit their sensitive temporary exclusion lists
PRIORITY AREA 3: ADDRESSING SUPPLY SIDE CONTRAINTS RELATED TO INFRASTRUCTURE		
Transport Facilitation Instrument	MS Implement the Transit Transport Facilitation Instruments	Harmonised Road Transit charges(HRTC) implemented by MS
		Harmonised Axle Load Limit implemented by MS
		Maximum Length 22.0m implemented by MS
		COMESA carrier Licence implemented by MS

		COMESA Transit Plates implemented by MS
		Overload Control Certificate implemented by MS
		Multidisciplinary Working Group (MWG) implemented by MS
		Yellow card adopted and used where applicable
	Implementation of the Yamoussoukro decision (YD) -Air Transport Liberalisation programme	Member States implement COMESA- legal notice no. 2 of 1999

OFFICIAL GAZETTE

of the

COMMON MARKET FOR EASTERN AND SOUTHERN AFRICA (COMESA)

Volume 16 No. 1

Issued on 15th October 2011

REVISED CHARTER FOR THE ESTABLISHMENT OF THE COMESA REGIONAL INVESTMENT AGENCY

CHARTER FOR THE ESTABLISHMENT

OF THE REGIONAL INVESTMENT AGENCY

TABLE OF CONTENTS

PREAMBLE

WHEREAS under Article 160 of the Treaty Establishing the Common Market for Eastern and Southern Africa (hereinafter referred to as "the Treaty"), COMESA Member States undertook to increase awareness of their investment incentives, opportunities, legislation, practices, major events affecting investments and other relevant information through regular dissemination and other awareness-promoting activities;

AND WHEREAS Member States recognise that for COMESA to effectively increase awareness of their investment incentives, opportunities, legislation, practices, major events affecting investments and other relevant information, it is necessary to establish a regional centre for regular dissemination of investment incentives, opportunities, legislation, practices, major events affecting investments and other relevant information;

TAKING INTO ACCOUNT the fact that approval for the establishment of the COMESA Regional Investment Agency was granted by the Authority of Heads of State and Government of COMESA in their Fourth Summit held in Nairobi, Kenya in May 1999;

COGNIZANT of the fact that at the Eighth Meeting of the Council of Ministers held in Lusaka, Zambia in November, 1999, Council noted the proposal of the Consultative Technical Meeting of Chief Executives of Investment Promotion Agencies to the effect *inter alia* that the COMESA Regional Investment Agency should not be a fully fledged agency but should start small, initially as an office or unit attached to the COMESA Secretariat, and should be allowed to evolve in due course, initially providing limited services, which could increase over time with a view to becoming self-sustaining through Member States contributions and other income generating activities;

NOTING that a Charter establishing the COMESA Regional Investment Agency was adopted at the Tenth Summit of the Authority in June, 2005 in Kigali, Rwanda;

REALISING the need to revise the COMESA Regional Investment Agency Charter that was adopted by the Authority in its Tenth Summit held in Kigali, Rwanda in June 2005;

NOW, THEREFORE, Council has decided to adopt this Revised Charter as follows:

PART I

INTRODUCTION

Article 1

Establishment of the Agency

1. The COMESA Regional Investment Agency in existence prior to the entry into force of this Charter shall be deemed to have been established under this Charter.

2. The Agency shall be an institution of COMESA situated in Cairo, in the Arab Republic of Egypt.

Article 2
Definitions

In this Charter, unless the context otherwise requires:

"**Agency**" means the COMESA Regional Investment Agency established by Article 1;

"**Authority**" means the Authority of COMESA established by Article 7 of the COMESA Treaty;

"**Board**" means the Board of Directors of the Regional Investment Agency established by Article 6;

"**Board Member**" means a member of the Board;

"**Charter"** means the Charter of the Agency;

"**COMESA**" means the Common Market for Eastern and Southern Africa;

"**Council**" means the Council of Ministers of COMESA established by Article 7 of the Treaty;

"**Country Unit**" means a body in a Member State, including a NIPA, dealing with investment matters;

"**Court**" means the Court of Justice of COMESA established by Article 7 of the Treaty;

"**Executive Director**" means the Executive Director of the Regional Investment Agency appointed under Article 6;

"**Member State**" means a Member State of COMESA;

"**NIPA**" means a National Promotion Investment Agency of a Member State;

"**Secretariat**" means the Secretariat of COMESA established by Article 7 of the Treaty;

"**Secretary General**" means the Secretary General of COMESA, as provided for by Article 17 of the Treaty;

"**Treaty**" means the Treaty Establishing the Common Market for Eastern and Southern Africa.

Article 3
Objectives of the Agency

The objectives of the Agency are to:

(a) Make COMESA the major destination for regional and international investors while simultaneously enhancing national investment; and

(b) Carry out other activities in the area of investment promotion, facilitation and advocacy in conformity with the Treaty.

Article 4
Functions of the Agency

1. The functions of the Agency shall be to do all that is necessary or expedient for the achievement of the objectives set out in Article 3.

2. Without prejudice to the generality of paragraph 1, the Agency shall be responsible for:

   (a) Gathering and disseminating information, including creating and maintaining a database and website on policies affecting the trade and investment environment, cost of doing business, trade procedures, investment procedures, investment and trade opportunities and other relevant information in Member States;

   (b) Proactively promoting and facilitating investment initiatives, policies and other issues in COMESA in conformity with the Treaty;

   (c) Identifying and promoting investment opportunities, with special focus on projects with a regional dimension;

   (d) Training and providing development support to NIPAs; and

   (e) Doing everything required for the fulfilment of or incidental to the abovementioned functions.

PART II

STRUCTURE AND ADMINISTRATION

Article 5

Structure of the Agency

There shall be established as organs of the Agency:

(a) The Council, which shall provide broad policy guidelines for the development and effective implementation of the objectives set out in Article 3; and

(b) The Board, which shall be responsible for the specific policy and direction of the Agency.

Article 6
Composition and Appointment of the Board

1. The Board shall be composed of seven (7) chief executive officers of NIPAs or experts of Member States. The Secretary-General or his representative shall be an ex-officio member of the Board.

2. Board Members shall be appointed by Council on the recommendation of the Secretary-General on such terms and conditions as Council may determine.

3. The Secretary-General shall make his recommendations from a list of chief executive officers of NIPAs or experts submitted by Member States.

4. The persons appointed as Board Members shall be reputable, with proven expertise and experience in the field of investment and trade or in other fields of activities directly or indirectly related to the activities of the Agency.

5. The number of Board Members may be modified by Council on the recommendation of the Secretary-General.

6. Board Members shall hold office for a term of two (2) years and may be eligible for re-appointment once.

7. In appointing Board Members, Council shall ensure that each Member State shall have an opportunity of serving on the Board and also ensure continuity through the reappointment of a number of serving Members.

8. A Board Member shall remain in office until a successor has been appointed.

9. A Board Member appointed in place of one whose office has become vacant before the end of his tenure shall hold office only for the remainder of that term.

10. The Executive Director and staff shall constitute the secretariat of the Board.

11. The Executive Director shall provide secretariat services to the Board.

Article 7
Functions of the Board

The Board shall:

(a) Act as an advisory body to the Council through the Secretary-General to ensure the proper functioning and development of the Agency in accordance with the Treaty and this Charter;

(b) Ensure the proper functioning and development of the Agency in accordance with the Treaty and this Charter;

(c) Make recommendations to Council on matters of policy regarding the proper functioning and development of the Agency;

(d) Submit to the Secretary-General, reports at such intervals as the Secretary-General may determine; and

(e) Exercise such other powers and perform such other duties as are conferred or imposed on it by this Charter, or as may from time to time be determined by the Secretary- General.

Article 8
Meetings of the Board

Subject to this Charter and any directions given by Council, the Board shall:

(a) Determine the frequency of its meetings; and

(b) Adopt its own procedure, including the conduct of business and the rotation of the position of the Chairperson among Board Members.

Article 9
Executive Director and Staff of the Agency

1. The Agency shall be headed by an Executive Director who shall be appointed by the Council on the recommendation of the Board, through the office of the Secretary-General, to serve for a term of three years, and shall be eligible for re-appointment for a further period of three years.

2. The Executive Director shall be the principal executive officer and shall be responsible for the operations of the Agency.

3. The Executive Director shall exercise the functions required to be performed under this Charter under the overall supervision of the Secretary-General.

4. There shall be such other staff of the Agency as Council may determine on the recommendation of the Board.

5. The terms and conditions of service of the Executive Director and other staff of the Agency shall be determined by the Council. Detailed terms and conditions of the Executive Director and staff shall be contained in staff rules and regulations to be adopted by the Council.

6. The Executive Director may be removed from office by the Council in accordance with the staff rules and regulations of the Agency.

7. In appointing staff to offices in the Agency, regard shall be had, subject to the importance of securing the highest standards of integrity, efficiency and the technical competence, to the desirability of maintaining an equitable distribution of appointments to such offices among citizens of all Member States.

8. In the performance of their duties, the Executive Director and staff of the Agency shall not seek or receive instructions from any Member State or from any other authority external to the Agency.

Article 10
Functions of the Executive Director

The Executive Director shall:

(a) Supervise the implementation of the policies made by Council;

(b) Submit regular reports on the activities of the Agency to the Board;

(c) Be responsible for the administrative and financial aspects of the Agency;

(d) On his own initiative, or as may be assigned to him by the Board, Council or the Secretary-General, undertake such work and studies and perform services related to the objectives of the Agency; and

(e) Collect information and verify matters of fact relating to the functioning of the Agency and for that purpose, may request Member States to provide information relating thereto.

Article 11
Independence of the Agency

1. Subject to other provisions of this Charter, in the performance of their duties, the Board Members, Executive Director and staff of the Agency shall refrain from any actions which might adversely reflect on their position as international officials responsible only to the Agency and other institutions of COMESA.

2. Member States undertake to respect the international character of the responsibilities of the Board Members, Executive Director and staff of the Agency and shall not seek to unduly influence them in the discharge of their responsibilities.

Article 12
Co-operation with other Institutions

The Agency may, with the prior approval of the Secretary-General, enter into contracts or arrangements with any other person, body or institution pursuing objectives similar to those of, or helpful to the Agency.

Article 13
Communication and Information

1. Each Member State shall designate a country unit with which the Agency may collaborate in pursuit of the objectives of this Charter.

2. The Member States agree to co-operate with and assist the Secretary- General and the Executive Director in the performance of the functions conferred upon them by this Charter and, in particular, to provide information relating to the activities of the Agency, which may be requested by them.

PART III

FINANCIAL RESOURCES AND AUDIT

Article 14
Budget

1. There shall be a budget for the Agency funded by annual contributions of the Member States and such other resources as may be determined by the Council.

2. The contributions of the Member States shall be based on the budget as approved by the Council on the recommendation of the Board, through the Secretary-General.

3. All expenditure of the Agency in respect of each financial year shall be approved by the Council as part of the budget of the Secretariat through the office of the Secretary-General on recommendation of the Board.

4. A draft budget for each financial year shall be prepared by the Executive Director and shall be approved by the Board for recommendation to the Council through the Secretary-General.

5. There may be special budgets to meet extraordinary expenditures of the Agency.

Article 15

Fees

The Agency may charge fees for any services rendered by it.

Article 16

Loans, Grants and Special Funds

The Agency may, through the Secretary-General, accept loans, grants and special funds and any other assistance:

Provided that the Agency shall not accept loans, grants, special funds or other assistance that may prejudice, limit, deflect or otherwise alter its objectives under this Charter.

Article 17
Application of Resources

The resources and facilities of the Agency shall be used to attain the objectives of the Agency as set out in this Charter.

Article 18
Reserve Funds

The Agency shall maintain a reserve fund into which any budgetary surplus in any financial year shall be deposited. The reserve fund shall be employed in such a manner and for such purposes as the Board may determine.

Article 19
Accounts of the Agency and External Auditors

1. The accounts of the Agency relating to each financial year shall be prepared in accordance with international accounting standards and shall be audited in the following financial year by external auditors appointed by Council under Article 169 of the Treaty.

2. The external auditors shall examine all documents and books of account relating to the operations and administration of the Agency and report thereon to the Board and Council.

Part IV
DISSOLUTION

Article 20
Termination of Operations

1. This Charter shall be of indefinite duration.

2. Notwithstanding the provisions of paragraph 1, the Authority may terminate the operations of the Agency.

3. After the operations of the Agency have been terminated, the Agency shall forthwith cease all activities except that incidental to orderly relations, the conservation and preservation of its assets and settlement of its obligations.

Article 21
Liability of Member States and Payment of Claims

1. In the event of the termination of operations of the Agency, the liability of the Member States for their share of contributions due shall continue until all claims of creditors, including all contingent claims, have been discharged.

2. All creditors holding direct claims shall first be paid out of the assets of the Agency and then out of contributions owing. Before making any payments to creditors holding direct claims, the Council shall make such arrangements as are necessary to ensure a pro-rata distribution among holders of direct and contingent claims.

Article 22
Distribution of Assets

1. No distribution of assets shall be made to Member States on account of their contributions to the budget until all liabilities to creditors have been discharged or provided for and any such

distribution shall be approved by the Council on the recommendation of the Board.

2. Any distribution of the assets of the Agency to Member States shall be in proportion to their contributions to the budget and shall be effected at such times and under such conditions as the Council considers fair and equitable. The shares of assets distributed need not be uniform as to type of asset. No Member State shall be entitled to receive its share in such a distribution of assets until it has settled all its obligations to the Agency.

3. Any Member State receiving assets distributed pursuant to this Article shall enjoy the same rights with respect to such assets as the Agency enjoyed prior to their distribution.

PART V

GENERAL PROVISIONS

Article 23
Official Languages

The official languages of the Agency shall be the official languages of COMESA.

Article 24
Status of the Agency

1. The Agency shall enjoy international legal personality.

2. The Agency shall have in the territory of the Arab Republic of Egypt, the:

   (a) Legal capacity required for the performance of its functions; and

   (b) Power to acquire or dispose of moveable and immovable property in accordance with the laws and regulations in force in the Arab Republic of Egypt.

3. The Agency shall, in the exercise of its legal personality, be represented by the Executive Director, or such other official as may be designated in writing by the Executive Director.

Article 25
Power to make Regulations

1. The Council may make regulations for carrying out the provisions of this Charter.

2. Without prejudice to the generality of paragraph 1, the Council shall make:

(a) Staff rules and regulations; and

(b) Financial regulations for the application of the provisions of Part III.

3. In the event of a conflict between this Charter and the Regulations, or Rules made thereunder, this Charter shall prevail.

Article 26
Supremacy of the Treaty

In the event of a conflict between this Charter and the Treaty, the provisions of the Treaty shall prevail.

Article 27

Amendment of the Charter

1. This Charter may be amended by the Council, on the recommendation of the Board, through the Secretary-General, in such manner as is prescribed in the Treaty with regards to the decision making process of Council.

2. When an amendment has been adopted, the Secretary-General shall certify it in a formal communication addressed to all Member States. Amendments shall enter into force three calendar months after the date on which such communication is issued, unless Council specifies a different period.

Article 28
Interpretation and Application

Any question of interpretation or application of the provisions of the Charter shall be submitted to the Board for decision.

Article 29
Settlement of Disputes

In the case of a dispute arising out of the application and interpretation of this Charter, such dispute shall be submitted to the COMESA Court of Justice for adjudication pursuant to Article 23(1) of the Treaty.

Article 30
Privileges and Immunities

1. After the entry into force of this Charter, any immunities and privileges extended to the Agency by the Government of the Arab Republic of Egypt prior to the entry into force of this Charter shall continue to be extended to the Agency.

2. Where necessary, the Executive Director shall enter into such additional agreements with the Government of the Arab Republic of Egypt relating to the privileges and immunities to be enjoyed by the Agency, the Executive Director and other eligible staff of the Agency.

3. While on official mission to Member States, the Board Members, the Executive Director and other eligible staff shall enjoy the same privileges and immunities as are enjoyed by officials of COMESA. For this purpose, the Member States hereby undertake, in their respective jurisdictions, to extend the application of the appropriate privileges and immunities accordingly.

4. The Executive Director and eligible staff of the Agency shall in all Member States enjoy diplomatic privileges and immunities no less favourable than those enjoyed by other international organisations.

Article 31
Savings

Any act or thing done, or document executed by the Agency in existence prior to the entry into force of this Charter, shall be deemed to have been so done or executed under this Charter; provided that such act or thing done, or document executed is not in any way inconsistent with the provisions of this Charter.

Article 32
Final Provisions

1. This Charter shall enter into force on the date of its adoption by Council

2. All Member States shall be members of the Agency.

3. The Charter shall be in all the official languages of COMESA in texts that are equally authentic and shall be deposited with the Secretary-General.

4. Once this Charter enters into force, the Secretary-General shall transmit certified copies thereof to Member States, Country Units and to such other international organisations as the Board may determine.

OFFICIAL GAZETTE

of the

COMMON MARKET FOR EASTERN AND SOUTHERN AFRICA (COMESA)

Volume 16 No. 2

Issued on 15th October 2011

CYBER CRIME MODEL BILL, 2011

CYBER CRIME MODEL BILL, 2011

TABLE OF CONTENTS

PREAMBLE

A Law to provide for a framework to combat cybercrime, the misuse of computers and to provide for offences and their prosecution; to enable the benefits of cyberspace and global connection to cyber networks to be enjoyed by all citizens; to facilitate a safe, secure and effective environment to conduct and use electronic communications and transactions; to promote legal certainty and confidence; to provide for the investigation, search and seizure of digital evidence; to provide for procedures for international cooperation, information sharing, and investigative assistance with law enforcement agencies including the extradition of persons; provide for a framework for national domain name space management; cryptography and authentication services; and consumer protection; and to provide for matters connected with or incidental to the foregoing.

PART I

PRELIMINARY

Section 1

Definitions

For purposes of this Law, unless the context otherwise requires:

"Access" means to make use of; to gain entry to; to view, display, instruct, or communicate with; to store data in or retrieve data from; to copy, move, add, change, or remove data; or otherwise make use of, configure, or reconfigure any resources of a computer program, computer, computer system, network, or their accessories or components, whether in whole or in part, including the logical, arithmetical, memory, transmission, data storage, processor, or memory functions of a computer, computer system, or network, whether by physical, virtual, direct, or indirect means or by electronic, magnetic, audio, optical, or other means.

"Communication Log" means a record of communication events in a certain scope, excluding the content of those communications, in order to provide an audit trail; that can be used to understand the activity of a system.

"Computer" means an electronic, magnetic, optical, electrochemical, or other data processing or communications device, or grouping or such devices, capable of performing logical, arithmetic, routing, or storage functions and which includes any storage facility or equipment or communications facility or equipment directly related to or operating in conjunction with such device(s), but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device.

"Computer Data" means any representation of facts, information, concepts, elements, state, or instructions in a form suitable for communications, interpretation, or processing in a computer programme or part of a programme, computer, or computer system, suitable to cause a computer programme, computer, computer system, or network to perform a function, process, and/or operation. Computer data shall include, but not be limited to: flowcharts,

architectures, programme hierarchies and interfaces, libraries, directories, topologies, taxonomies, process flows, internal controls, and metadata.

"Computer Programme" means a set of coded instructions, whether in machine readable or human readable formats (source code or object code), that enables a computer, computer system, and/or network to process computer data, traffic data, and/or content data to cause such computer, computer system, and/or network to perform a function and/or operation.

"Computer System" means a computer, physical or virtual, or collection of such computers and any components and/or accessories, temporarily or permanently interconnected or related, and one or more of which contain computer programmes, computer data, content data, and/or traffic data, in whatever form, that perform functions, including, but not limited to: logic, arithmetic, information creation, storage, sorting, copying, changing, retrieval, destruction, routing**,** communications, and/or control.

"Content Data" means any data whether in digital, optical, or other form, including metadata, that conveys essence, substance, information, meaning, purpose, intent, or intelligence, either singularly or when in a combined form, in either its unprocessed or processed form. Content data includes any data that conveys the meaning or substance of a communication as well as data processed, stored, or transmitted by computer programmes.

"Critical Infrastructure" means the computers, computer systems, and/or networks, whether physical or virtual, and/or the computer programmes, computer data, content data and/or traffic data so vital to this country that the incapacity or destruction of or interference with such systems and assets would have a debilitating impact on security, national or economic security, national public health and safety, or any combination of those matters.

"Cyberspace" means the physical and non-physical terrain created by and/or composed of some or all of the following: computers, computer systems, networks, and their computer programmes, computer data, content data, traffic data, and users.

"Damage" means any disruption, interception, interference, and/or destruction of computer data, content data, traffic data, a computer programme, computer, computer system, or network, including the transmission and/or receipt of computer data, content data, or traffic data by a computer programme, computer, computer system, or network.

"Data" means electronic representations of information in any form.

"Data message" means information generated, sent, received or stored by electronic, magnetic, optical or similar means, including, but not limited to: electronic data interchange, electronic mail, telegram, telex or telecopy.

"Disruption" means an event that causes a computer programme, computer, computer system, network, or component thereof, to be inoperable, or operate in an unintended manner, for a length of time due to destruction of and/or interference with a computer programme, computer, computer system, network, computer data, content data, and/or traffic data.

"Electronic communication" means any communication that the parties make by means of data messages.

"Information system" means a system for generating, sending, receiving, storing or otherwise processing data messages.

"Interception" means the acquisition, viewing, capture, or copying of the contents or a portion thereof, of any communication, including content data, computer data, traffic data, and/or electronic emissions thereof, whether by wire, wireless, electronic, optical, magnetic, oral, or other means, during transmission through the use of any electronic, mechanical, optical, wave, electromechanical, or other device.

"Interference" means:

i. Hindering, blocking, impeding, interrupting, or impairing the processing of, functioning of, access to, or confidentiality, integrity, or availability of a computer programme, computer, computer system, network, computer data, content data, or traffic data by inputting, transmitting, damaging, deleting, destroying, deteriorating, altering, or suppressing computer data, content data, traffic data, a computer programme, computer, computer system, or network; and/or

ii. Corrupting, damaging, deleting, deteriorating, altering, or suppressing a computer programme, computer data, content data, or traffic data.

"Loss" means any reasonable costs, including, but not limited to, the cost of responding to an offense under this Law, conducting an investigation or damage assessment, and/or the cost of analyzing, restoring, replacing, or reproducing computer data, content data, traffic data, a computer programme, computer, computer system, or network to its condition prior to the offense, and/or other consequential damages incurred by an individual or entity arising from damage, interference, disruption, interception and/or the destruction of computer data, content data, traffic data, a computer programme, computer, computer system, network, and/or other information.

"Malware" means a programme that is inserted into a computer programme, computer, or computer system, with the intent of compromising the confidentiality, integrity, or availability of the computer programme, computer, computer system, network, computer data, content data, or traffic data or of otherwise disrupting the beneficial use thereof.

"Network" means a group of computers or computer systems of whatever form, topology, or functionality that is connected at points (nodes) which have the capability to transmit, receive, share, or forward information, communication signals, and operational instructions.

"Service Provider" means:

i. Any public or private entity that provides to users of its service the ability to communicate by means of a computer programme, computer, computer system, or network, including the services that support the development or utilization of computer programmes and/or the creation, storage, retrieval, processing, management, and deletion of computer data, traffic data, and content data; and/or

ii. Any other entity that processes or stores computer data, content data, or traffic data on behalf of such service (as set forth in (i) of this paragraph) or users of such service.

"Subscriber Information" means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services, other than traffic data or content data, and by which can be established:

i. The type of communication service used, the technical provisions taken thereto, and the period of service;

ii. The subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, as it is available on the basis of the service agreement or arrangement; and/or

iii. Any information regarding the location of installed communications equipment as disclosed in the service agreement or arrangement.

"Traffic Data" means any computer or other data relating to a communication by means of a computer programme, computer, computer system, or network, generated by a computer programme, computer, computer system, or network that formed a part in the chain of communication, indicating the communication's origin, destination, route, format, intent, time, date, size, duration, or type of underlying service. Packet headers or pen register and shall include trap and trace data.

PART II

SUBSTANTIVE PROVISIONS

Section 2

Legal Recognition of Electronic Communications

1. A communication or a contract shall not be denied validity or enforceability on the sole ground that it is in the form of an electronic communication.

2. This, in this Law, shall not be construed as;

(a) Requiring a party to use or accept electronic communications, record, retain, store or display any information, document or signature, by, or in, electronic form; or

(b) Prohibiting a person from establishing requirements in respect of the manner in which that person will accept data messages;

(c) This Law does not limit the operation of any law that specifically authorizes, prohibits or regulates the use of data messages, including any requirement by, or under, any law for information to be posted or displayed in a specific manner, or for any information or document to be transmitted by a specific method.

Section 3

Form Requirements

1. Where the law requires that a communication or a contract should be in writing, or provides consequences for the absence of writing, that requirement is met by an electronic communication if the information contained therein is accessible so as to be usable for subsequent reference.

2. Where the law requires that a communication or a contract should be signed by a party, or provides consequences for the absence of a signature, that requirement is met in relation to an electronic communication if:

(a) A method is used to identify the party and to indicate that party's intention in respect of the information contained in the electronic communication; and

(b) The method used is either:

i. As reliable and appropriate for the purpose for which the electronic communication was generated or communicated, in the light of all the circumstances, including any relevant agreement; or

ii. Proven in fact to have fulfilled the functions described in sub-paragraph (a) above, by itself or together with further evidence.

3. Where the law requires that a communication or a contract should be made available or retained in its original form, or provides consequences for the absence of an original, that requirement is met in relation to an electronic communication if:

(a) There exists a reliable assurance as to the integrity of the information it contains from the time when it was first generated in its final form, as an electronic communication or otherwise; and

(b) Where it is required that the information it contains be made available, that information is capable of being displayed to the person to whom it is to be made available.

4. For the purposes of paragraph 3(a):

(a) The criteria for assessing integrity shall be whether the information has remained complete and

unaltered, apart from the addition of any endorsement and any change that arises in the normal course of communication, storage and display; and

(b) The standard of reliability required shall be assessed in light of the purpose for which the information was generated and in light of all the relevant circumstances.

5. Where a seal is required by law to be affixed to a document and such law does not prescribe the method or form by which such document may be sealed by electronic means, that requirement shall be met if the document indicates that it is required to be under seal and it includes the advanced electronic signature of the person by whom it is required to be sealed.

6. Where any law requires or permits a person to send a document or information by registered or certified post or similar service, that requirement shall be met if an electronic copy of the document or information is sent to the post office, is registered by the post office and sent by that post office to the electronic address provided by the sender.

7. An expression in a law, whether used as a noun or verb, including the words “document”, “record”, “file”, “submit”, “lodge”, “deliver”, “issue”, “publish”, “write in”, “print” or words or expression of similar effect, shall be interpreted so as to include or permit such form, format or action in relation to any information contained in the electronic communication unless otherwise provided for in this Law.

Section IV

Time and Place of Dispatch and Receipt of Electronic Communications

1. The time of dispatch of an electronic communication is the time when it leaves an information system under the control of the originator or of the party who sent it on behalf of the originator or, if the electronic communication has not left an information system under the control of the originator or of the party who sent it on behalf of the originator, the time when the electronic communication is received.

2. The time of receipt of an electronic communication is the time when it becomes capable of being retrieved by the addressee at an electronic address designated by the addressee. The time of receipt of an electronic communication at another electronic address of the addressee is the time when it becomes capable of being retrieved by the addressee at that address and the addressee becomes aware that the electronic communication has been sent to that address. An electronic communication is presumed to be capable of being retrieved by the addressee when it reaches the addressee’s electronic address.

3. An electronic communication is deemed to be dispatched at the place where the originator has its place of business and is deemed to be received at the place where the addressee has its place of business, as determined in accordance with paragraph (2).

4. Paragraph (s) of this section applies notwithstanding that the place where the information system supporting an electronic address is located may be different from the place where the electronic communication is deemed to be received under paragraph (3) of this section.

Section V

Admissibility and Evidential Weight of Data Messages or Documents Established by Electronic Means

1. In any legal proceedings, nothing in the application of the rules of evidence shall apply so as to deny the admissibility of a data message in evidence:

(a) (i.) On the sole ground that it is a data message; or,
(ii) If it is the best evidence that the person adducing it could reasonably be expected to obtain, on the grounds that it is not in its original form.

(b) In assessing the evidential weight of a data message, regard shall be had to the reliability of the manner in which the integrity of the information was obtained, to the manner in which its originator was identified and to any other relevant factor.

(c) A copy or any other reproduction of documents established by electronic means shall have the same evidentiary weight as the document itself when it is certified accurate by bodies approved by a competent authority.

2. Securing electronic records:

Where a prescribed security procedure, or a commercially reasonable security procedure agreed to by the parties involved, has been properly applied to an electronic record to verify that the electronic record has not been altered since a specified point in time, the record shall be treated as a secure electronic record from such specified point in time to the time of verification.

3. Certificates:

Any person relying on a digital signature shall also rely on a valid certificate containing the public key by which the digital signature can be verified and issued in accordance with the prescribed rules under this Law.

4. Confidentiality:

No person who has, pursuant to any power conferred under this Part, obtained access to an electronic record, book, register, correspondence, information, document or other material shall disclose such electronic record, book, register, correspondence, information, document or other material to any other person except for the purposes of this Act or as required under a written law.

5. Production of documents and data:

The competent authority may -

(a)Require the production of records, accounts, data and documents kept by a certification authority and inspect, examine and take copies of any of them;

(b) Require the production of an identification document from any person in relation to any offence under this Act;

(c) Make such inquiry as may be necessary to ascertain whether this Act has been complied with.

PART III

CONSUMER PROTECTION

Section 6

Information to be provided by Supplier

1. A supplier offering goods or services for sale, hire or exchange by way of electronic communication shall make the following information available to consumers on the website where the goods or services are offered:

i. Its full names and legal status;
ii. Its physical address and telephone number;
iii. Its website address and e-mail address;
iv. Membership of any self-regulatory or accreditation bodies to which that supplier belongs or subscribes and the contact details of that body;
v. Any code of conduct to which that supplier subscribes and how that supplier subscribes and how that code of conduct may be accessed electronically by the consumer;
vi. In the case of a legal person, its registration number, the names of its registration number, the names of its office bearers and its place of registration;
vii. The physical address where that supplier will receive legal service of documents;
viii. A sufficient description of the main characteristics of the goods or services offered by that supplier to enable a consumer to make an informed decision on the proposed electronic transaction;
ix. The full price of the goods or services, including transport costs, taxes and any other fees or costs;
x. The manner of payment for the goods or services;
xi. Any terms of agreement, including any guarantees, that will apply to the transaction and how those terms may be accessed, stored and reproduced electronically by consumers;
xii. The time within which the goods will be dispatched or delivered or within which the services will be rendered;
xiii. The manner and period within which consumers can access and maintain a full record of the transaction;
xiv. The return, exchange and refund policy of that supplier;
xv. Any alternative dispute resolution code to which that supplier subscribes and how the wording of that code may be accessed electronically by the consumer;
xvi. The security procedures and privacy policy of that supplier in respect of payment, payment information and personal information;
xvii. Where appropriate, the minimum duration of the agreement in the case of agreements for the supply of products or services to be performed on an ongoing basis or recurrently; and
xviii. The rights of consumers in terms of Section 7, where applicable.

2. A supplier shall provide a consumer with an opportunity to:

(a) Review the entire electronic transaction;
(b) Correct any mistakes; and
(c) Withdraw from the transaction, before finally placing any order.

3. If a supplier fails to comply with the provisions of paragraph (1) or (2), the consumer may cancel the transaction within fourteen days of receiving the goods or services under the transaction.
4. If a transaction is cancelled under paragraph (3)

(a) The consumer shall return the goods of the supplier or, where applicable, cease using the services performed; and

(b) The supplier shall refund all payments made by the consumer minus the direct cost of returning the goods.

5. A supplier shall use a payment system that is sufficiently secure in accordance with accepted technological standards at the time of the transaction and the type of transaction concerned.

6. A supplier is liable for any damage suffered by a consumer due to the failure by the supplier to comply with paragraph (5).

Section 7

Cooling – Off Period

1. A consumer may cancel, without giving any reason and without incurring any penalty, a transaction and a related credit agreement for the supply -

(a) Of goods, within seven days after the date of the receipt of the goods; or
(b) Of services, within a period of seven days after the date of the conclusion of the agreement.
(c) Where a consumer cancels a transaction under sub-section (b), the only charge that may be levied on the consumer is the direct cost of returning the goods.

2. If payment for the goods or services has been effected prior to a consumer exercising the right referred to in sub-section (b), the supplier shall give the consumer a full refund of the payment, which refund shall be made within a period of thirty days of the date of cancellation.

3. This section shall not be construed as prejudicing the rights of a consumer provided for in any other law.

Section 8

Performance

1. A supplier shall execute an order within a period of thirty days from the date on which the supplier receives the order, unless the parties have agreed otherwise.

2. Where a supplier has failed to execute an order within a period of thirty days or within the agreed period, the consumer may cancel the agreement upon giving a period of seven days written notice.

3. Where a supplier is unable to perform under the agreement on the grounds that the goods or services ordered are unavailable, the supplier shall immediately notify the consumer of this fact and refund any payments within thirty days after the date of notification.

Section 9

Non- Exclusion

Any provision in an agreement, which excludes any rights provided for in this Part, is null and void.

Section 10

Consumer Complaints

A consumer may lodge a complaint with the competent authority in respect of any non-compliance with the provisions of this Part by a supplier.

PART IV

National Domain Name, Cryptography and Authentication Services and Related Matters

Section 11

Domain Name, Cryptography and Authentication Service Administration

The competent authority [ies] shall administer and manage:

(a) The domain name space for this country and in doing so -

(i) Licence and regulate registries and registers for the registries;
(ii) Publish rules on the general administration and management of the domain name space for this country; and
(iii) Comply with international best practice.

(b) The provision of cryptography services or products and accreditation of authentication services in this country within the prescribed rules, including but not limited to the registration to provide the services, public access to the database in respect of such services, and the status of the registration or accreditation.

(c) Computer incident response teams responsible for the prevention, detection, and recovery from incidents including but not limited to the co-ordination of incident handling activities, analyzing threats, vulnerabilities and other information, the dissemination of such information to relevant persons, and the establishment of standards and best practices for relevant authority approval;

(d) Compliance, enforcement and dispute resolution of matters falling under this Law including: electronic commerce and taxation, standards, quality of service, information security auditing, and intellectual property; and

(e) Protection and privacy of data including the storage and availability of data to third parties, and raising of awareness of users of data and electronic communication networks in general, within the prescribed rules, and in doing so shall comply with international best practice.

PART V

Limitation of Liability of Service Providers

Section 12

Definition of Service Provider

1. In this Part, “service provider” means any person providing information system services.

2.A service provider is not liable for providing access to, or for operating facilities for, information systems or transmitting, routing or storage of data messages through an information system under the service provider's control, as long as the service provider:

i. Does not initiate the transmission;

ii. Does not select the addressee;
iii. Performs the functions in an automatic, technical manner without selection of the data; and
iv. Does not modify the data contained in the transmission.

3. The acts of transmission, routing and provision of access referred to in paragraph (i) include the automatic, intermediate and transient storage of the information transmitted in so far as this takes place –

(a) For the sole purpose of carrying out the transmission in the information system;
(b) In a manner that makes it ordinarily inaccessible to anyone other than anticipated recipients; and
(c) For a period no longer than is reasonably necessary for the transmission.

4. A legal authority may order a service provider to terminate or prevent any unlawful activities under this Law or any other law.

Section 13

Caching

1. A service provider that transmits data provided by a recipient of the service through an information system under the service provider's control shall not be liable for the automatic, intermediate and temporary storage of that data, where the purpose of storing such data is to make the onward transmission of the data more efficient to other recipients of the service upon their request, as long as the service provider -

(a) Does not modify the data;
(b) Complies with conditions or guidelines issued by competent authorities on access, and maintenance of the integrity of the data;
(c) A legal authority may order a service provider to terminate or prevent any unlawful activities under this Law or any other law.

Section 14

Hosting

1. A provider of a service consisting of the storage of data provided by a recipient of the service, shall not be liable for damages arising from data stored at the request of the recipient of the service, as long as the service provider -

(a) Does not have actual knowledge that the data message, or an activity relating to the data message, is infringing the rights of a third party;

(b) Is not aware of facts or circumstances from which the infringing activity or the infringing nature of the data message is apparent; and

(c) Upon receipt of a take-down notification acts expeditiously to remove or to disable access to the data.

2. Paragraph (1) shall not apply where the recipient of the service is acting under the authority or the control of the service provider.

3. A legal authority may order a service provider to terminate or prevent any unlawful activities under this Act or any other law.

Section 15

Use of Information Location Tools by Service Provider

1. A service provider shall not be liable for any damage incurred by a person if the service provider refers or links users to a web page containing an infringing data message or infringing activity, by using information location tools, including a directory, index, reference, pointer, or hyper link, and where the service provider-

(a) Does not have actual knowledge that the data message or an activity relating to the data message is infringing the rights of that person;
(b) Is not aware of facts or circumstances from which the infringing activity or the nature of the data message is apparent;
(c) Does not receive a financial benefit directly attributable to the infringing activity; and
(d) Removes, or disables access to, the reference or link to the data message or activity within a reasonable time after being informed that the data message or the activity relating to that data message, infringes the rights of a person.

Section 16

Take-Down Notification

1. The recipient of a service may, through a take-down notification, notify the service provider of -

(a) Any data or activity infringing the rights of the recipient or of a third party;
(b) Any unlawful material or activity; or
(c) Any other matter conducted or provided contrary to the provisions of this Law.

2. A take-down notification shall include information prescribed by the legal authority.
3. Any person who lodges a false take-down notification with a service provider shall have committed a criminal offense punishable by a fine of [amount]_____ and/or imprisonment for a period of _____.

Section 17

No General Obligation on Service Provider to Monitor Unlawful Activities

1. Subject to the other provisions of this Part, a service provider shall not be under any obligation to -

(a) Monitor the data which the service provider transmits or stores; or
(b) Actively seek facts or circumstances indicating an unlawful activity.

2. The competent authority may prescribe procedures for service provider's to -

(a) Inform the competent public authorities of alleged illegal activities under-taken, or information provided, by recipients of their service; and

(b) Communicate to the competent authorities, at their request, information enabling the identification of recipients of their service.

PART VI

Acts against Computers, Computer Systems, Networks, Computer Data, Content Data, and Traffic Data

Section 18
Unauthorized Access to Computers, Computer Systems, and Networks

1. A person who, without authorization or in excess of authorization or by infringement of security measures, intentionally accesses in whole or in part, a computer, a computer system and/or connected system, or a network, with the intention of conducting any activity within the definition of "Access" in this Law and which is prohibited under this Law shall have committed a criminal offense punishable by a fine of [amount]_____ and/or imprisonment for a period of _____.

2. A person who gains unauthorized access pursuant to paragraph (1) of this section to a computer, computer system and/or connected system, or network that is exclusively for the use of the Government of this country, or in the case where such is not exclusively for the use of the Government but is used by or on behalf of the Government of the country and such conduct is intended to affect that use or impact the operations of the Government of the country, shall have committed a criminal offense punishable by a fine of [amount]_____ and/or imprisonment for a period of _____.

3. A person who gains unauthorized access pursuant to paragraph (1) of this section to a computer, computer system and/or connected system, or network that is exclusively for the use of critical infrastructure operations, or in the case where such is not exclusively for the use of critical infrastructure operations but the computer, computer system and/or connected system, or network is used for critical infrastructure operations and such conduct is intended to affect that use or impact the operations of critical infrastructure, shall have committed a criminal offense punishable by a fine of [amount]_____ and/or imprisonment for a period of _____.

4. A person who gains unauthorized access pursuant to paragraph (1) of this section when such conduct is with the intention of developing, formulating, planning, facilitating, assisting, informing, conspiring, or committing acts of terrorism, not limited to acts of cyber terrorism, shall have committed a criminal offense punishable by a fine of [amount]_____ and imprisonment for a period of _____.

Section 19

Unauthorized Access to Computer Programs, Computer Data, Content Data, Traffic Data

1. A person who, without authorization or in excess of authorization or by infringement of security measures, intentionally accesses in whole or in part:

   (a) A computer programme,
   (b) Computer data,
   (c) Content data, or
   (d) Traffic data,

With the intention of conducting any activity within the definition of "access" in this Law and which is prohibited under this Law shall have committed a criminal offense punishable by a fine of [amount]_____ and/or imprisonment for a period of _____.

2. A person who gains unauthorized access pursuant to paragraph (1) of this section to a computer program, computer data, content data, or traffic data that has been

determined by the Government of this country, pursuant to law or decree, to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any other reason pertaining to national or economic security, shall have committed a criminal offence, punishable by a fine of [amount]_____ and imprisonment for a period of _____, irrespective of whether or not such programme or data was communicated, delivered, or transmitted to any person not entitled to receive it or retained by the person who accessed it.

3. A person who gains unauthorized access pursuant to paragraph (1) of this section to a computer program, computer data, content data, or traffic data that is used, processed, or stored by any ministry, agency, department, office, or entity of the Government of this country and such data or programme is exclusively for the use of the Government of this country, or in the case in which such data or programme is not exclusively for the use of the Government but it is used by or on behalf of the Government, and such conduct is intended to affect that use or impact the operations of the Government of this country, shall have committed a criminal offence punishable by a fine of [amount] _____ and/or imprisonment of _____.

4. A person who gains unauthorized access pursuant to paragraph (1) of this section to a computer programme, content data, computer data, or traffic data that is exclusively for the use of critical infrastructure operations, or in the case in which such is not exclusively for the use of critical infrastructure operations, but the programme or data is used in critical infrastructure operations and such conduct is intended to affect that use or impact the operations of critical infrastructure, shall have committed a criminal offence, punishable by a fine of [amount]_____ and imprisonment of _____.

5. A person who gains unauthorized access pursuant to paragraph (1) of this section and such conduct is with the intention of:

(a) Accessing or acquiring financial data of a financial institution, or
(b) Facilitating, advancing, assisting, conspiring, or committing extortion, identity theft, or any other illegal act not covered by provisions within this Law, whether or not via a computer programme, computer, computer system, or network, shall have committed a criminal offence, punishable by a fine of [amount]_____ and/or imprisonment of _____.

6. A person who gains unauthorized access and/or acquisition pursuant to paragraph (1) of this section and such conduct is with the intention of developing, formulating, planning, facilitating, assisting, informing, conspiring, or committing acts of terrorism, not limited to acts of cyber terrorism, shall have committed a criminal offence punishable by a [amount]_____ fine and imprisonment for a period of _____.

7. A person who transmits any unsolicited electronic information to another person for purposes of illegal trade or commerce or other illegal activity, shall have committed a criminal offense punishable by a fine of [amount]_____ and/or imprisonment for a period of _____ years, or to both.

Section 20

Interference or Disruption

1. A person who, without authorization or in excess of authorization or by infringement of security measures, intentionally causes interference or disruption of a computer, computer system and/or connected systems, or networks shall have committed a criminal offense punishable by a fine of [amount]_____ and/or imprisonment for a period of _____.

2. A person who, without authorization or in excess of authorization or by infringement of security measures, intentionally causes interference or disruption of a computer programme, computer data, content data, or traffic data shall have committed a criminal offense punishable by a fine of [amount]_____ and/or imprisonment for a period of _____.

3. A person who commits interference or disruption pursuant to paragraphs (1) or (2) of this section with the intent to cause or with knowledge that such conduct could cause serious harm to life, limb, or property or threaten public health and/or safety, shall have committed a criminal offense punishable by a fine of [amount]_____ and/or imprisonment for a period of _____.

4. A person who commits interference or disruption pursuant to paragraphs (1) or (2) of this section with the intent to cause or with knowledge that such conduct could cause interference and/or disruption of computers, computer systems and/or connected systems, networks, computer programmes, computer data, content data, or traffic data used by the Government in furtherance of the administration of justice, national security, or national defense shall have committed a criminal offense punishable by a fine of [amount]_____ and imprisonment for a period of _____.

5. A person who commits interference or disruption pursuant to paragraphs (1) and (2) of this section with the intent to cause or with knowledge that such conduct could cause interference and/or disruption of the computers, computer systems and/or connected systems, networks, computer programmes, computer data, content data, or traffic data used by critical infrastructure, shall have committed a criminal offense punishable by a fine of [amount]_____ and imprisonment for a period of _____.

6. A person who commits interference or disruption pursuant to paragraphs (1) and (2) of this section with the intent of developing, formulating, planning, facilitating, assisting, informing, conspiring, or committing acts of terrorism, not limited to acts of cyber terrorism, shall have committed a criminal offense punishable by a fine of [amount]_____ and imprisonment for a period of _____.

Section 21

Interception

1. A person who intentionally and without authorization pursuant to the rules of criminal procedure and any other laws of this country, intercepts, by technical means, transmissions of non-public computer data, content data, or traffic data, including electromagnetic emissions or signals from a computer, computer system, or network carrying or emitting such, to or from a computer, computer system and/or connected system, or network shall have committed a criminal offense punishable by a fine of [amount]_____ and/or imprisonment for a period of _____.

Section 22

Misuse and Malware

1. A person who intentionally and without authorization causes the transmission of a computer programme, information, code, or command with the intent of causing damage to a network, computer, computer system and/or connected system, computer, computer programme, content data, computer data, or traffic data shall have committed a criminal offense punishable by a fine of [amount]_____ and/or imprisonment for a period of _____.

2. A person who intentionally and without authorization engages in the production, sale, or procurement for use, import, distribution, or otherwise makes available:

(a) A computer or computer programme, designed or adapted primarily for the purpose of committing any of the offenses provided for in Sections 2 to 5; and/or

(b) A computer password, access code, command, instruction, or similar data by which the whole or part of any computer, computer system, network, computer programme, computer data, content data, or traffic data may be accessed, with the intent that it be used for the purpose of committing any of the offenses provided for in Sections 2 to 5 shall have committed a criminal offense punishable by a fine of [amount]_____ and/or imprisonment for a period of _____.

3. A person who is in possession of one or more items referred to in (a) and (b) of paragraph (2) of this section with the intent that they be used for the purpose of committing any of the offenses provided for in sections 2 to 5 shall have committed a criminal offense punishable by a fine of [amount]_____ and/or imprisonment for a period of _____.

4. Notwithstanding the foregoing, this Section shall not be interpreted to impose criminal liability where the production, sale, procurement for use, import, distribution, or otherwise making available or possession of the items referenced in (a) and (b) of paragraph (2) of this section is not for the purpose of committing any of the offenses provided for in Sections 2 to 5, such as for the authorized testing or protection of computer systems and data.

5. A person who commits an offense under paragraphs (1) or (2) of this Section with the intent to cause or with the knowledge that such conduct could cause physical injury to any person shall be punished by a fine of [amount]_____ and/or imprisonment for a period of _____.

6. A person who commits an offense under paragraphs (1) or (2) of this Section with the intent to cause or with the knowledge that such conduct could cause the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of one or more individuals shall be punished by a fine of [amount]_____ and/or imprisonment for a period of _____.

7. A person who commits an offense under paragraph (1) of this Section with the intent to cause or with the knowledge that such conduct could cause a threat to public safety or public health shall be punished by a fine of [amount]_____ and/or imprisonment for a period of _____.

8. A person who commits an offense under paragraph (1) of this Section with the intent of developing, formulating, planning, facilitating, assisting, informing, conspiring, or committing acts of terrorism, not limited to cyber terrorism, shall be punished by a fine of [amount]_____ and imprisonment for a period of_____.

Section 23

Digital Forgery

1. A person who intentionally and without authorization or legal right, engages in the input, acquisition, alteration, deletion, or suppression of a computer programme, computer data, content data, or traffic data or otherwise alters the authenticity or integrity of such programme or data, with the intent that it be considered or acted upon for legal purposes as though it were authentic or with integrity, regardless of whether or not the programme or data is directly readable or intelligible, for any unlawful purpose, shall have committed a

criminal offense punishable by a fine of [amount]_____ and/or imprisonment for a period of _____.

Section 24

Digital Fraud, Procure Economic Benefit

1. A person who knowingly and with intent to defraud, transfers, or otherwise disposes of, to another, or obtains control of with the intent to transfer or dispose of a computer password, access code, or similar data by which the whole or part of any computer programme, computer, computer system, network, computer data, content data, or traffic data may be accessed shall have committed a criminal offense punishable by a fine of [amount] _____ and/or imprisonment for a period of _____.

2. A person who intentionally and without authorization or legal right causes the loss of property to another person through:

(a) The input, acquisition, alteration, deletion, or suppression of a computer program, computer data, content data, or traffic data; or

(b) The interference with the functioning of a computer, computer system and/or connected system, or network; with the fraudulent or dishonest intent to procure an economic benefit for oneself or another shall have committed a criminal offense punishable by a fine of [amount] _____ and/or imprisonment for a period of _____.

Section 25

Extortion

1. A person who knowingly transmits any communication containing any threat to cause damage to a computer, computer system and/or connected system, network, computer programme, computer data, content data, or traffic data with the intent to extort from any person any money or other thing of value shall have committed a criminal offense punishable by a fine of [amount] _____ and/or imprisonment for a period of _____.

Section 26

Aiding, Abetting, and Attempting

1. A person who knowingly and intentionally aids or abets the commission of any of the offenses provided for in Sections 18 to 25 shall have committed a criminal offense punishable by a fine of [amount]_____ and imprisonment for a period of _____.

2. A person who knowingly and intentionally attempts to commit any of the offenses provided for in Sections 18 to 25 shall have committed a criminal offense punishable by a fine of [amount]_____ and imprisonment for a period of _____.

Section 27

Corporate Liability

1. Any legal person (corporation, association, or other legal entity) may be subject to civil, criminal, or administrative penalties for any offense provided for in Sections 18 to 26 if:

(a) The offense was committed by a person holding a leading position in the legal person;
(b) The leading person acted

i. On his/her authority to represent the legal person;
ii. On the authority vested in him/her to make decisions on behalf of the legal person, or
iii. In his/her authority to exercise control within the legal person; and

(c) The offense was committed for the benefit of the legal person.

2. Any legal person may be subject to civil, criminal, or administrative penalties for any offense provided for in Sections 18 to 26 if:

(a) The offense was committed by an employee or agent of the legal person who was acting within the scope of his authority;
(b) The offense was committed for the benefit of the legal person; and
(c) The commission of the offense was made possible by the negligence of a leading person that resulted in the failure to supervise the employee or agent through appropriate and reasonable measures intended to prevent employees or agents from committing criminal activities on behalf of the legal person.

3. Liability under paragraphs (1) and (2) of this Section shall be without prejudice to the criminal liability of the natural person who has committed the offense.

PART VII

PROCEDURAL PROVISIONS FOR CRIMINAL INVESTIGATIONS AND PROCEEDINGS FOR OFFENSES

Section 28
Scope of Procedural Provisions

1. his part shall apply to specific criminal investigations or proceedings arising from offenses prohibited by Part ii and Sections 18 to 26 of this Law and/or the laws of other jurisdictions that prohibit the same or similar actions.

2. Except as provided otherwise in Section 5, pertaining to the interception of computer data, content data, or traffic data, these provisions apply to:

(a) The criminal offenses provided for in Section 18 to 26 of this Law;
(b) Other criminal offenses committed by means of a computer, computer system, or network; and
(c) The collection of evidence in electronic form relating to such offenses.

Section 29

Retention of Data on Communication Logs

1. A service provider shall retain data on communication logs in its original form for the purpose of investigating, detecting and prosecuting crime for a minimum period of six months.

Section 30

Retention of Electronic Records

1. Where any law provides that documents, records or information shall be retained for any specific period, then that requirement shall be deemed to have been satisfied where such documents, records or information are retained in electronic form if:

(a) The information contained therein remains accessible so as to be usable for subsequent reference;

(b) The electronic record is retained in the format in which it was originally generated, sent or received or in a format which can be demonstrated to represent accurately the information originally generated, sent or received; and

(c) The details which will facilitate the identification of the original destination, date and time of dispatch or receipt of such electronic record are available in the electronic record -

Provided that this clause shall not apply to any information which is automatically generated solely for the purpose of enabling an electronic record to be dispatched or received.

Section 31

Retention of Information in Original Form

1. Where any law requires information to be presented or retained in its original form, that requirement is met by an electronic record if:

(a) There exists a reliable assurance as to the integrity of the information from the time when it was first generated in its final for as an electronic message or otherwise; and

(b) Where it is required that information be presented, that information is capable of being displayed to the person to whom it is to be presented.

2. Sub-section (1) applies whether the requirement therein is in the form of an obligation or whether the law simply provides consequences for the information not being presented or retained in its original form.

3. For the purposes of sub-section (1)(*a*):

(a) The criteria for assessing integrity shall be whether the information has remained complete and unaltered, apart from the addition of any endorsement and any change which arises in the normal course of communication, storage and display; and

(b) The standard of reliability required shall be assessed in the light of the purpose for which the information was generated and in light of all the relevant circumstances.

Section 32

Conditions and Safeguards

1. The procedural provisions set forth in Part VII of this Law are subject to:

(a) The conditions and safeguards provided elsewhere in the Laws of this country, including, but not limited to, judicial or other independent supervision, grounds justifying application, and limitation on the scope and duration of such power or procedure.

(b) The conditions and safeguards concerning human rights and liberties guaranteed under the laws of this country; and

(c) International instruments, treaties, and laws, including the 1966 United Nations International Covenant on Civil and Political Rights.

2.

(a) The procedural provisions set forth in this Part shall be conducted in compliance with the principal of proportionality, and be abided by in all criminal investigation activities performed by competent law enforcement bodies whenever evidence is to be gathered on and/or by means of electronic tools.

(b)Criminal investigation activities include, but are not limited to: inspections, searches, seizure, custody, urgent inquiries, and searches for evidence.

(c) The impact of these procedural powers upon the rights, responsibilities, and legitimate interests of third parties alien to the facts investigated shall be considered when conducting investigative activities.

Section 33

Preservation of Stored Computer Data, Content Data, Traffic Data

1. The rules of criminal procedure for this country shall enable competent authorities to order or similarly obtain the expeditious preservation of specified computer data, content data, and/or traffic data that has been or may be stored by means of a computer or computer system, when there are grounds to believe that such data is particularly vulnerable to loss or modification.

2. Where an order is issued to a person to preserve specified computer data, content data, or traffic data in a person's possession or control, that person shall preserve and maintain the integrity of such data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities of this country or of another jurisdiction to seek its disclosure.

3. The integrity of such preserved data shall be documented, including the method used to determining such integrity, which may include but not be limited to: the use of a mathematical algorithm and resulting hash, and such record maintained along with the preserved data.

4. Competent authorities may request that the preservation order be renewed.

5. The custodian and any other person ordered to preserve such data shall keep confidential all information regarding such order for the period of time specified by the order or required under the Laws of this country.

6. The provisions of this Section are subject to the provisions of Sections 28 and 32 of this Law.

Section 34

Expedited Preservation and Partial Disclosure of Traffic Data

1. The rules of criminal procedure for this country shall provide:

(a) For the expedited preservation of specified traffic data by a competent authority in this country, irrespective of whether one or more service providers are involved in the transmission of the subject communications; and

(c) The disclosure to competent authorities, or a designate of such authority, of a sufficient amount of traffic data to enable the identification of the service providers and the path through which the communication was transmitted.

2. The provisions of this Section are subject to the provisions of Sections 28 and 32 of this law.

Section 35

Expedited Preservation of Computers or Storage Media

1. The rules of criminal procedure for this country shall enable competent authorities to order or obtain the expeditious preservation of specified computers or storage media in situations in which there is an investigative, forensic, or practical necessity to do so to protect and preserve the computing environment to enable the extraction and examination of data and computing instructions, particularly when there are grounds to believe that such data is particularly vulnerable to loss or modification or when the preserving entity lacks the requisite capability to safely and effectively preserve the computing and/or content data external to the computer or storage media.

2. Where an order is issued to a person to preserve specified computers and/or storage media in the person's possession or control, that person shall preserve and maintain the integrity of such computers and/or storage media for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities of this country or of another jurisdiction to seek its disclosure.

3. Competent authorities may request that a preservation order be renewed.

4. The person and custodian ordered to preserve such computers and/or storage media shall keep confidential all information regarding such order for the period of time specified by the order.

5. The provisions of this Section are subject to the provisions of Sections 28 and 32 of this Law.

Section 36

Production Order

1. The rules of criminal procedure for this country shall enable a competent authority to order:

(a) A person to submit specified computer data, content data, and/or traffic data in that person's possession or control, which is stored in a computer, computer system, or a computer data storage medium; and

(b) A service provider offering services in this country to submit specified subscriber information relating to such services that is in that service provider's possession or control.

2. The provisions of this Section are subject to the provisions of Sections 28 and 32.

Section 37

Search and Seizure of Stored Data

1. The rules of criminal procedure for this country shall enable competent authorities, upon adequate reason and within the scope of legal approval, to search or similarly access:

(a) A specified computer, computer system, computer program, or parts thereof, and/or the computer data, content data, and/or traffic data stored therein; and

(b) A computer data storage medium on which computer data, content data, or traffic data may be stored in this country.

2. When the authorities seeking approval to conduct a search pursuant to paragraph (1) of this Section have grounds to believe that the data sought is stored in another computer system, or part of another system in this country, which is

owned by or under the control of the same entity for which the scope of legal approval was granted, and such data is lawfully accessible from or available to the initial system, the rules of criminal procedure shall enable the authorities to expeditiously extend the search or similar accessing to the other system.

3. The rules of criminal procedure for this country shall enable competent authorities to seize or similarly secure computer data, content data, or traffic data accessed pursuant to paragraphs (1) and (2) of this Section, including the power to:

(a) Seize or similarly secure a computer or computer system, or part of it, or a computer data storage medium;

(b) Make and retain an image or copy of the computer data, content data, or traffic data;

(c) Maintain the integrity of the relevant stored data and document such integrity by means of a mathematical algorithm, which shall be maintained along with the stored computer data; and

(d) Render inaccessible or remove those computer data in the accessed computer system.

4. The competent authority [ies] in this country may order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs (1) and (2) of this Section.

5. The provisions of this Section are subject to the provisions of Sections 28 and 32 of this Law.

Section 38

Interception (Real-Time Collection) of Traffic Data

1. The competent authority [ies] of this country may, upon adequate reason and within the scope of legal approval:

(a) Collect or record traffic data in real-time through technical means;

(b) Compel a service provider, within its existing capability, to collect or record such traffic data in real-time or to cooperate and assist the competent authorities in the collection and recording of traffic data associated with the specified communications in this country transmitted by means of a computer system and/or network.

2. Any service provider requested to collect and record such traffic data in real-time or to cooperate or assist with such shall keep confidential the fact of the request and any information related to it.

3. The provisions of this Section are subject to the provisions of Sections 12 and 13 of this Law.

Section 39

Interception (Real-Time Collection) of Content Data

1. The competent authority [ies] of this country may, upon adequate reason and within the scope of legal approval, collect or record through technical means, or compel a service provider, within its existing technical capability, to collect or record or to cooperate and assist the competent authorities in the collection and recording of content data, in real-time, of specified communications transmitted by means of a computer system.

(a) Any service provider requested to collect and record such content data in real-time or to cooperate or assist with such shall keep confidential the fact of the request and any information related to it.

(b) The provisions of this Section are subject to the provisions of Sections 28 and 32 of this Law.

PART VIII

JURISDICTIONAL PROVISIONS

Section 40

Jurisdiction

1. The competent authority [ies] of this country shall have jurisdiction over any person, irrespective of his nationality or citizenship, who commits any offense established pursuant to Sections 18 through 26 of this Law, when the offense is committed -

(a) Within the territory of this country; or
(b) Using equipment, software, or data located within this country, regardless of the location of the perpetrator, or
(c) Directed against equipment, software, or data located in this country, regardless of the location of the perpetrator.

2. The competent authority [ies] of this country shall have jurisdiction over offenses committed pursuant to Sections 18 to 26 of this Law if the offense is committed -

(a) On board a ship flying the flag of this country; or
(b) On board an aircraft registered under the Laws of this country.

3. The competent authority [ies] of this country shall have jurisdiction over offenses committed pursuant to Sections 18 to 26 of this Law if the offense is committed by a citizen or resident of this country, and -

(a) If the offense is punishable under criminal law where it was committed; or
(b) If the offense is committed outside the territorial jurisdiction of any country.

4. In instances where an alleged offender is present in this country and this country elects to refuse a request for extradition of the alleged offender to another country on the basis of his or her nationality, jurisdiction over the stated offences shall be established in this country.

5. When another country claims jurisdiction over an offense within Sections 18 to 26 of this Law, the officials of the countries involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for the prosecution of the offense.

6. An offense is committed at every place the perpetrator acted -

   (a) Through his or her physical presence;
   (b) Through the intentional use of equipment, software, or data; or
   (c) At any location where the resulting action is an element of an offense pursuant to Sections 18 to 26 of this Law occurred or would have occurred according to the understanding of the perpetrator.

7. In specific cases, this country may reserve the right to apply or not to apply the jurisdictional rules in paragraphs (2) and (3) of this Section.

PART IX

INTERNATIONAL CO-OPERATION

Section 41

International Cooperation: General Principles

1. The legal authorities of this country shall cooperate directly and to the widest extent possible with legal authorities of another country and/or with international organizations specializing in criminal matters for purposes of:

(a) Investigations or proceedings concerning criminal offenses related to computer programmes, computers, computer systems, networks, computer data, content data, and/or traffic data; and/or

(b) The collection of evidence in electronic or any other form of a criminal offense. Such cooperation shall take place under the conditions of this Law and by observing -

i. The obligations that this country has assumed under international legal instruments on cooperation in criminal matters that this country is party to;

ii. Arrangements agreed upon on the basis of uniform or reciprocal legislation in this regard; and

iii. The laws of this country.

2. The co-operation, organization and investigations carried out according to paragraph (1) of this Section, may pertain to, as appropriate:

(a) International legal assistance in criminal matters;

(b) Extradition;

(c) The identification, blocking, seizing or confiscation of the evidence, products, and instruments of the criminal offence;

(d) The carrying out of common investigations, including but not limited to, the place where the perpetrator physically typed the command on a computer, the place where equipment or software intentionally used or attacked by the perpetrator is located, and locations where the perpetrator thought the attack or action would impact;

(e) The exchange of information;

(f) Technical assistance or assistance of any other nature for the collection of information;

(g) Specialized personnel training; and

(h) Other such activities deemed appropriate.

Section 42

Extradition Principles

1. This Section applies to extradition between this country and another country, irrespective to whether there is an extradition treaty between this country and the requesting country, for the criminal offenses committed pursuant to Sections 18 to 26 of this Law, provided that they are punishable under the laws of both countries and require deprivation of liberty for a maximum period of one year or longer.
2. Notwithstanding the provisions of this Law, where the authorities of this country and another country agree on a different minimum penalty based upon uniform or reciprocal legislation or an extradition treaty, including the European Convention on Extradition (ETS No. 24), applicable between

the countries, the minimum penalty provided for under such agreement or treaty shall apply.

3. The criminal offenses provided for in Sections 18 to 26 of this Law shall be deemed as extraditable offenses under any extradition treaty or agreement to which this country is a party and under all future treaties pertaining to extradition.

4. If extradition for a criminal offense pursuant to Sections 18 to 26 of this Law is refused solely on the basis of the nationality of the person sought or because this country desires to have jurisdiction over the offense, the competent legal authorities of this country shall submit the case to the appropriate authorities in this country for the purpose of prosecution and shall report the outcome to the requesting country in due course.

Section 43

Mutual Assistance: General Principles

1. (a) The competent authority [ies] of this country shall provide assistance to another country to the widest extent possible for the purpose of investigations or proceedings concerning the criminal offenses established pursuant to Sections 18 to 26 of this Law and for the collection of evidence in electronic or other form.

(b)The rules of criminal procedure shall be amended to the extent necessary to support this requirement, including the procedures pertaining to mutual assistance requests in the absence of applicable international agreements.

2. Requests for and responses to requests for expedited mutual assistance may be made to the authorities of this country via the most efficient means, including facsimile or electronic mail, provided that appropriate levels of authentication and security are utilized and formal confirmation follows the request or response. The competent officials of this country shall respond to such requests by any such expedited means of communication.

3. Mutual assistance shall be provided in accordance with this Law or other Laws of this country or by mutual assistance treaties to which this country is bound, including the grounds on which cooperation may be refused. Such assistance shall not be refused with respect to offenses pursuant to Sections 18 through 26 solely on the grounds that the request concerns a fiscal offense.

4. Where mutual assistance from this country requires the existence of dual criminality, that condition shall be deemed fulfilled by this Law, irrespective of whether the offense in this country is in the same category of offenses or within the same terminology as the requesting country's law, provided that the offense is a criminal offense under the laws of the requesting country.

Section44

Unsolicited Information

1. The legal authority [ies] of this country may forward to another country information obtained within its own investigations when it considers that the disclosure of such information may -

(a) Assist the other country in initiating or carrying out investigations or proceedings concerning criminal offenses similar to those provided for in to Sections 18 to 26 of this Law; or

(b) Might lead to further cooperation with that country.

2. Prior to providing such information, the legal authorities of this country may subject the data to confidentiality requirements or other conditions, but shall not forward such

information unless such requirements or conditions are accepted by the other country.

Section 45

Procedures for Mutual Assistance

1. The provisions of this Section shall apply where there is no mutual assistance treaty or reciprocal or uniform law between the requesting country and this country.

2. Where there is a mutual assistance treaty or reciprocal or uniform law between the requesting country and this country, the provisions of this Section may apply upon mutual agreement of this country and the requesting country.

3. The rules of criminal procedure for this country shall specify a central authority responsible for sending and answering requests for mutual assistance, execute such requests, and or transmit requests to the appropriate authorities competent for their execution, and communicate with similar authorities in requesting countries.

4. Mutual assistance requests shall be handled according to the procedures of the requesting country unless they are incompatible with the rules of criminal procedure of this country, in which case the rules of this country shall take precedence.

5. The central authority responsible for sending and answering requests for mutual assistance may refuse to provide mutual assistance if:

(a) Such request is against the laws of this country, except refusal shall not be allowed for offenses within Sections 18 to 26 of the Law on the grounds that they are considered a fiscal offense;

(b) Such request concerns an offense which the competent authorities of this country consider a political offense or an offense connected to a political offense; or

(c) Execution of the request is likely to prejudice the sovereignty of this country, its security, public order and safety, or other essential interests.

(d) The central authority may postpone action on a mutual assistance request if such action would prejudice criminal or investigations or proceedings within this country, and in dealing with the matter, the central authority shall first consider whether the request may be partially granted or subjected to conditions.

6. The rules of criminal procedure shall establish a process for the central authority to promptly inform the requesting country of the outcome of any requests for assistance, with reasons provided for postponement, refusal, or circumstances which would delay the assistance or render it impossible.

7. The central authority shall:

(a) Keep confidential the fact of the request and its subject, if so requested by the requesting country, except to the extent necessary to execute the request, or

(b) Provide an explanation to the requesting country why such confidentiality is not possible to enable the requesting country to determine if the request should be nevertheless executed.

8. Urgent requests for mutual assistance or requests not involving coercive action may be sent:

(a) Directly by judicial authorities of the requesting country to the competent [judicial authority] of this country, with a copy of such request sent to the central authorities of both countries,

understanding that the [judicial authority] of this country may, in its discretion, refer the matter to the central authority; or

(b) To the International Criminal Police Organization (Interpol), with a copy of such request sent to the central authority.

9. This requested information may be supplied upon the condition that it be kept confidential or that it shall not be used for investigations or proceedings other than those stated in the request.

10. If the requesting country cannot comply with such conditions, the [legal authorities] in this country shall determine whether the requested information shall nevertheless be provided and the central authority shall communicate such decision to the requesting country. The competent authorities in this country supplying any such information shall require the receiving party to abide by any confidentiality requirements and to provide an explanation regarding the use made of the information provided.

Section 46

Expedited Preservation of Stored Computer Data, Content Data, or Traffic Data

1. Within mutual assistance, the competent authorities of a country may request the expeditious preservation of specified computer data, content data, or traffic data located within the territory of this country, in respect of which the requesting country intends to submit a request for mutual assistance for the search or for access, seizure, or similar securing or disclosure of the data.

2. The request for expedited preservation referred to in paragraph (1) of this Section shall specify:

(a) The authority requesting the preservation;

(b) The offense that is the subject of a criminal investigation or proceeding and a brief statement of the related facts;

(c) The stored computer data, content data, and/or traffic data to be preserved and its relationship to the offense;

(d) Any available information identifying the custodian of such stored data or the location of the computer or computer system(s) containing the data;

(e) The necessity of the preservation; and

(f) That the requesting country intends to submit a request for mutual assistance for the search or for access, seizure, or similar securing or disclosure of the subject data.

3. Upon receipt of such a request, the competent authorities of this country shall take all appropriate measures to preserve expeditiously the specified data in accordance with the Laws of this country. Dual criminality shall not be required for such preservation.

4. A request for preservation may only be refused if the request concerns an offense that this country considers a political offense or an offense connected with such, or this country determines that the execution of the request is likely to prejudice its sovereignty, security, public safety, or other essential interests.

5. Where the competent legal authority [ies] believe that the requested preservation will not ensure the future availability of the data or will threaten the confidentiality or otherwise prejudice the other country's investigation, the legal authority [ies] shall promptly inform the requesting country, which may then determine if the preservation should nevertheless be executed.

6. No preservation effected under this Section shall be for a period of less than sixty (60) days to enable the requesting country to submit a request for the search or similar access,

seizure or similar securing, or disclosure of the data. Following the receipt of such request, the data shall continue to be preserved pending a decision on the request.

Section 47

Expedited Disclosure of Preserved Content Data, Computer Data, or Traffic Data

1. If, in executing a request for preservation according to Section 43 of this Law, the legal authority [ies] of this country discover that a service provider in another country was involved in the transmission of the communication, the legal authority [ies] shall promptly disclose to the requesting country a sufficient amount of traffic data to identify that service provider and the path through which the communication was transmitted.

2. Disclosure of traffic data, as prescribed by paragraph (a) of this Section, may only be withheld from the requesting country if:

(a) The request concerns an offense that this country considers a political offense or an offense connected with such an offense; or

(b) The legal authorities of this country consider that the execution of the request is likely to prejudice its sovereignty, security, public safety, or other essential interests.

Section 48

Mutual Assistance Regarding Access to Stored Computer Data, Content Data, or Traffic Data

1. The competent officials of another country may request the competent officials of this country to search or similarly access, seize or similarly secure, and disclose specified data stored by means of a computer or computer system located within the territory of this country, including data that has been preserved pursuant to Section 46of this Law. Such requests shall adhere to the principles pertaining to international cooperation in Section 38 of this Law and shall comply with other relevant provisions of this Law.

2. Requests pursuant to paragraph (1) of this Section shall be responded to on an expedited basis where -

(a) There are grounds to believe that the requested data is particularly vulnerable to loss or modification; or
(b) Expedited co-operation is provided according to the instruments, arrangements, and laws referred to in Section 38 of this Law.

Section 49

Trans-Border Access to Stored Computer Data, Content Data, or Traffic Data

1. A competent authority may access publicly available (open source) stored computer data, content data, or traffic data regardless of where the data is located geographically.

2. A competent authority from another country may, without authorization of authorities of this country, have access to and receive, by means of a computer or computer system located on its territory, specified computer data, content data, or traffic data stored in this country if the competent

authority from the other country obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to such competent authority through that computer or computer system.

Section 50

Mutual Assistance in Real-Time Collection of Traffic Data

1. The competent authorities of this country shall provide mutual assistance to the competent authorities of another country with respect to the real-time collection of specified traffic data associated with specified communications in the territory of this country that were transmitted by means of a computer or computer system. Subject to the provisions of paragraph (b) of this Section, this assistance shall be governed by the Laws and rules of criminal procedure for this country.

2. The competent authorities of this country shall provide assistance pursuant to paragraph (a) of this Section for criminal cases in a manner equal to that which would be available in a similar domestic case.

Section 51

Mutual Assistance Regarding Interception of Content Data or Computer Data

1. The competent authorities of this country shall provide mutual assistance to the competent authorities of another country in the real-time collection or recording of specified computer data or content data of specified communications transmitted by means of a computer or computer system to the extent permitted under the Laws of this country and treaties to which this country is bound.

Section 52

Points of Contact

1. The competent authorities of this country shall designate points of contact available on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offenses related to computers, computer systems, networks, computer data, content data, and/or traffic data, or for the collection of other evidence in electronic form related to a criminal offense. Such assistance shall include facilitating, or if permitted under the Laws of this country and the practices of competent authorities, directly carrying out the following measures:

(a) The provision of technical advice;
(b) The preservation of data pursuant to Sections 46 and 47; and
(c) The collection of evidence, the provision of legal information, and locating of suspects.

2. The points of contact shall have the capacity to carry out communications with the points of contact in other countries on an expedited basis. If the designated points of contact are not responsible for international cooperation and mutual assistance or extradition, the points of contact shall ensure that they are able to coordinate with such authorities on an expedited basis.

3. The competent authorities of this country shall ensure that all points of contact are properly trained and equipped or that other trained personnel are available to the points of contact to facilitate the operation of the network and compliance with the provisions of this Law.

PART X

PROVISIONS APPLICABLE TO OTHER OFFENSES

Section 53

Provisions That Apply to Other Offenses

1. The competent authorities of this country may, upon adequate reason and within the scope of legal approval and the Laws of this country and/or any legal obligations that this country may be subject to through -

(a) The Bern Convention for the Protection of Literary and Artistic Works;
(b) The Agreement on Trade-Related Aspects of Intellectual Property Rights;
(c) The WIPO Copyright Treaty;
(d) The International Convention for the Protection of Performers, Producers, Phonograms, and Broadcasting Organization;
(e) The WIPO Performance and Phonograms Treaty, and/or
(f) Any international agreements or treaties pertaining to child pornography -

May exercise the authority granted in Sections 28 to 51 of this Law to investigate or assist in the investigation of offenses related to such Laws or legal obligations.

2. The provisions of this Section are subject to the Provisions of Sections 28 and 32 of this Law.

Section 54

General penalty

A person who commits an offence under this Law for which no penalty has been provided shall be liable upon conviction to a maximum fine of [amount]_____ and/or imprisonment for a maximum period of _____

References:

1. Council of Europe Convention on Cybercrime
2. Commonwealth Model Law on Computer and Computer Related Crime
3. Draft Stanford Convention
4. Commonwealth Draft Model Law On Electronic Evidence
5. ITU Toolkit for Cybercrime Legislation
6. United Nations Convention on the Use of Electronic Communications in International Contracts (2005)
7. Council of Europe Convention on Cybercrime, available at: http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm
8. Commonwealth Model Law on Computer and Computer Related Crime, available at: http://www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf
9. Draft Stanford Convention, available at: http://www.stanford.edu/~gwilson/Transnatl.Dimension.Cyber.Crime.2001.p.249.pdf
10. http://www.itu.int/net/itunews/issues/2011/03/45.aspx