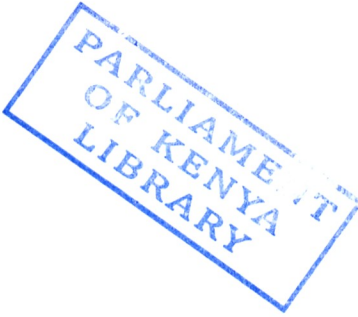


Approved for tabling,
~~Paul~~ SNA
25/10/18

PARLIAMENT OF KENYA



Paper led by the
Chairperson, Committee
on Information, Communication
and Innovation
MP
Tuesday 25/10/2018

THE NATIONAL ASSEMBLY

TWELFTH PARLIAMENT – SECOND SESSION – 2018

DEPARTMENTAL COMMITTEE ON INFORMATION, COMMUNICATION AND
INNOVATION

REPORT ON THE NATIONAL BROADCASTERS SHOW HELD IN LAS
VEGAS, NEVADA, USA FROM 7TH -12TH APRIL 2018.

DIRECTORATE OF COMMITTEE SERVICES,
CLERK'S CHAMBERS
PARLIAMENT BUILDINGS
NAIROBI

OCTOBER, 2018

ABBREVIATIONS..... 3

CHAIR’S FOREWORD 3

EXECUTIVE SUMMARY..... 5

PREFACE 1

1.1. Mandate of the Committee..... 1

1.2. Members of the Committee..... 2

1.3. Committee Secretariat 3

1.4. OBJECTIVES OF THE SHOW..... 4

1.5. COMPOSTION OF THE DELEGATION..... 4

2.0. INTRODUCTION..... 5

3.0. INFORMATION TECHNOLOGY SECURITY 6

3.1. Cyber Security..... 6

4.0. OBSERVATIONS 9

5.0. RECOMMENDATIONS 1

ABBREVIATIONS

NAB - National Broadcasters Show

NARTB -National Association and Television Broadcasters

IT - Information Technology

CISO -Chief Information Security Officers

ICT -Information Communication and Technology

FOREWORD BY THE LEADER OF THE DELEGATION

The show's tagline was '**Where content comes to life**'. It's is the largest tagline for media entertainment and technology and covers Broadcast Tv, Radio, data storage and data management.

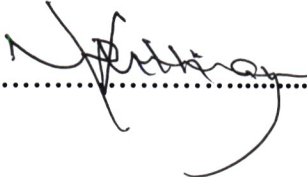
The purpose of the event was to give attendees an opportunity to appraise them with new trending technologies specifically on matters cyber security and IT governance.

The Show further highlighted the importance of digital technology in supporting Governments' efforts and an enabler in the realization of Vision 2030 and the big four agenda.

The meeting comes in the backdrop of various bills on Cyber security that are before the Committee, and with advancement in technology it is important that Parliament enacts legislation on information retention and privacy, to protect institutions against significant threats of information systems disruptions from hackers, worms, viruses and terrorists. The threats posed have resulted in a need for a governance approach to information management, protecting the organization's most critical assets and its information.

The Committee wishes to thank the office of the Speaker and Clerk of the National assembly for the support accorded to it before and during this event.

On behalf of the Committee and pursuant to provisions of the Standing Orders of the National Assembly, it is therefore my pleasant duty and privilege, to lay this report.

SIGN..........DATE.....11 / 10 / 2018

**HON. WILLIAM KISANG, MP- CHAIRPERSON
DEPARTMENTAL COMMITTEE ON COMMUNICATION, INFORMATION AND
INNOVATION.**

EXECUTIVE SUMMARY

Cybersecurity has been gaining attention as a national issue for the past decade. During this time, governments has witnessed cyber incidents affecting both public and private sector systems and data. These incidents have included attacks in which data was stolen, altered, or access to it was disrupted or denied.

The frequency of these attacks, and their effects on the economy, national security, and people's lives have driven cybersecurity issues to the forefront of governments policy conversations.

From a policymaking standpoint, cybersecurity includes the security of the devices, infrastructure, data, and users that make up cyberspace. The elements of ensuring cybersecurity involves policies spanning a range of fields, including education, workforce management, investment, entrepreneurship, and research and development.

Software development, law enforcement, intelligence, incident response, and national defense are involved in the response when something goes awry in cyberspace. To help secure and respond to incidents in cyberspace, agencies carry out their authorized responsibilities, run programs, and work with the private sector.

While every Government has a role in protecting its own data and systems, certain agencies have significant responsibilities with regard to national cybersecurity. The Department of Security secures ,coordinates critical infrastructure protection efforts, responds to cyber threats, investigates cybercrimes, funds cybersecurity research and development and promotes cybersecurity education and awareness.

This report covers a variety of topics related to cybersecurity in order to provide context and a framework for further discussion on selected policy areas,it also provides an overview of cybersecurity concepts that maybe of interest to the Kenyan Government

PREFACE

1.1. Mandate of the Committee

The Departmental Committee on Communications, Information and Innovation is established under *Standing Order 216* whose mandate pursuant to the Standing Order 216 (5) is as follows;

- a. Investigate, inquire into, and report on all matters relating to the mandate, management, activities, administration, operations and estimates of the assigned Ministries and departments;
- b. Study the programme and policy objectives of Ministries and departments and the effectiveness of the implementation;
- c. Study and review all legislation referred to it;
- d. Study, assess and analyze the relative success of the Ministries and departments as measured by the results obtained as compared with their stated objectives;
- e. Investigate and inquire into all matters relating to the assigned Ministries and departments as they may deem necessary, and as may be referred to them by the House;
- f. To vet and report on all appointments where the Constitution or any law requires the National Assembly to approve, except those under Standing Order 204 (*Committee on Appointments*);
- f (a) examine treaties, agreements and conventions;
- g. make reports and recommendations to the House as often as possible, including recommendation of proposed legislation;
- h. make reports and recommendations to the House as often as possible, including recommendation of proposed legislation;
- i. consider reports of Commissions and Independent Offices submitted to the House pursuant to the provisions of Article 254 of the Constitution; and

- j. Examine any questions raised by Members on a matter within its mandate.

In accordance with the Second Schedule of the National Assembly Standing Orders, the Committee is mandated to oversee Communication, Information, media and broadcasting (except for broadcast of parliamentary proceedings), Information Communications Technology (ICT) development and advancement of technology and modernization of production strategies.

1.2. Members of the Committee

The committee comprises of: -

1. Hon. Kisang William Kipkemoi, M.P - **Chairperson**
2. Hon. George Macharia Kariuki, M.P - **Vice Chairperson**
3. Hon. Liza, Chelule Chepkorir, M.P.
4. Hon. Alfah, O. Miruka, M.P.
5. Hon. Annie Wanjiku Kibeh, M.P.
6. Hon. Joshua Kimilu, Kivinda, M.P.
7. Hon. Marwa Kitayama Maisori, M.P.
8. Hon. Mwambu Mabongah, M.P.
9. Hon. Maritim Sylvanus, M.P.
10. Hon. Mwangaza Kawira, M.P.
11. Hon. Jonah Mburu, M.P.
12. Hon. Gertrude Mbeyu Mwanyanje, M.P.
13. Hon. Wamuchomba, Gathoni, M.P.
14. Hon. (Eng)Mark Nyamita Ogola, M.P
15. Hon. John Kiarie Waweru, M.P.
16. Hon. Erastus Nzioka Kivasu, M.P.
17. Hon. Innocent Momanyi, Obiri, M.P.
18. Hon. Godfrey Osotsi, Atieno, M.P.
19. Hon. Anthony, Tom Oluoch, M.P.

1.3. Committee Secretariat

The Ccommittee Secretariat comprises of:-

1. Mr. Nicholas Emejen - Deputy Director Committee Services
2. Ms. Ella Kendi - Third Clerk Assistant
3. Mr. Ronald Walala - Legal Counsel II
4. Ms. Lorna Okatch - Research Officer
5. Ms. Catherine Burure - Fiscal Analyst
6. Ms. Deborah Mupusi - Media Relations Officer
7. Mr. Wilson Angatangoria - Serjeant at arms



1.4. OBJECTIVES OF THE SHOW

The show was aimed to: -

- a) Promote cyber security leadership and governance from the top level of every Government and organization.
- b) Identify gaps and build capacity for strategic, technical and operational elements of cyber security.
- c) Identify mechanisms that will provide guidance and protect critical assets by coordinating efforts to respond to and recover national cyber incidents.

1.5. COMPOSTION OF THE DELEGATION

The delegation comprised of the following members and a staff: -

1. The Hon. Kisang William,MP- Chairperson/ **Leader of Delegation**
2. The Hon. Gertrude Mbeyu Mwanyanje, M.P
3. The Hon.Jonah Mburu, M.P.
4. The Hon. Mark Nyamita Ogola,MP
5. The Hon. Wamuchomba, Gathoni, M.P.
6. Ms. Angeline Naserian Lotuai – **Delegation Secretary**

10
11
12

13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100

2.0. INTRODUCTION

The NAB was founded as the National Association of Radio Broadcasters (NARB) in April 1923 in Chicago, USA. The association's founder and first president were Eugene Fc Mac Donald who also launched the Zenith Corporation. In 1951 it changed its name to the National Association of Radio and Television Broadcasters (NARTB) to include the television industry. In 1958 it adopted its current name National Association of Broadcasters.

The NAB worked to establish a commercial radio system in the United States. The system was set up in August 1928 with the establishment of General Order 40, a radio reallocation scheme by the Federal Radio commission which awarded the choicest frequencies and broadcast times to the then-emerging commercial radio industry.

The main aim of National Broadcasters Show is to set up and provide a ground-breaking technology and innovation solutions.

The show highlighted and emphasized on cyber security, this has led to an increased need to focus on the overall value of information protection and delivery of enabled services. Organizations today face a global revolution in governance that directly affects their information management practices.

Due to the high-profile organizational failures of the past decade, legislatures, statutory authorities and regulators have created a complex array of new laws and regulations designed to force improvement in organizational governance, security, controls and transparency.

It was said that new laws on information retention and privacy, coupled with significant threats of information systems disruptions from hackers, worms, viruses and terrorists, have resulted in a need for a governance approach to information management, protecting the organization's most critical assets and its information and reputation.

To achieve effectiveness and sustainability in today's complex and interconnected world, information security must be addressed at the highest levels of the organization, not to be regarded as a technical specialty relegated to the IT department.

3.0. INFORMATION TECHNOLOGY SECURITY

3.1. Cyber Security

It was showcased that Cyber security or information technology security which are the techniques of protecting computers, networks, programs and data from unauthorized access or attacks that are aimed exploitation.

Cybersecurity issues are gaining national prominence, generating extensive media coverage and affecting organizations nationwide. The frequency of cybersecurity incidents and their effects on the economies has elevated Governments' interest in cybersecurity issues.

It was also emphasized that the world is changing rapidly, and cyber threats are becoming more frequent and severe. Most cyber-attacks are automated and indiscriminate, exploiting known vulnerabilities rather than targeting specific organizations.

Information security is not only a technical issue, but a business and governance challenge that involves adequate risk management, reporting and accountability. Effective security requires the active involvement of executives to assess emerging threats and the organization's response to them.

Large scale cyber-attacks are becoming more frequent and costlier for businesses and organizations. Attackers are better funded and better organized than in the past. Dozens of banks have suffered cyber-attacks at the hands of foreign attackers.

As technology becomes more integrated in our day lives and a supporting pillar of the global economy, the cybersecurity skills shortage is becoming more critical and broadly recognized. The threat of cybercrime looms large for every industry including Broadcasting.

It was said that there is shortage of specialist in matters cyber security and a rash of cyber-attacks is spurring companies who don't have CISO to hire them. Top talent is coming from governments such as National Security agencies, public sector is experiencing its own shortage as more of its talent joins private sector.

To salvage the situation Governments should consider their recruitment strategy for these professionals and make it clear to education institutions that there are career prospects in this exciting space.

For sure, internet is a great source of creativity and innovation, it has fostered vivid storytelling and has given audiences new ways to enjoy those stories. In the recent events, it is clear that criminals are also using it to steal trade and content and Organizations of all forces are vulnerable to this kind of menace. Governments and private sectors are faced with the monumental task of defending against these criminal activities.

The internet is a key driver of trade in intellectual property related trade however, it can render infringement of intellectual property rights easier and identify those responsible from infringement more challenging. Therefore, better security is not going to come cheap, organizations will have to boost allocations on cyber-security spending. It is worth noting that organizations adopt cloud, mobile and social computing because information technology environments are becoming more difficult to defend.

Increasingly, organizations need to accept that security breaches are inevitable and need to go beyond defense to include detection, response and recovery. All these things give rise to a need to new skills, approaches and specialized tools and services, including continuous monitoring and threat forensic powered analytics.

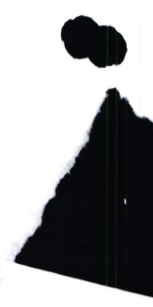
It was said that most organizations believe that their information security systems are secure, often the reality is that they are not.

There are two important trends that can help organizations stay ahead of threats: -

1. Collective Intelligence

The distributed and involving nature of cyber-attacks and threats calls for collaborative and networked defense. In the context of cyber security, collective intelligence refers to the sharing of information about vulnerability, threats and remedies between enterprises and governments. Collective intelligence can improve risk management by quickly spreading knowledge of vulnerabilities and threats.

100



100

It can direct security audits and cyber forensics to areas of known or suspected weaknesses. And it can reveal trends and suggest areas where investments in additional security measures is warranted. Therefore, promoting the sharing of cyber threats and vulnerability information between the public and private sectors as key aim.

2. Technology Professional Services

It was highlighted that with cloud, mobile and social computing, creating new security vulnerabilities, traditionally security products such as firewalls and anti-virus scanners cannot thwart every threat. Tools such as network security analyzers can be difficult to effectively employ without outside help and specialized cyber security talents.

Organizations are responding by introducing security offerings that marry the automation and analytical capabilities with human intelligence. Such technological offerings can help monitor, collect and analyze large data sets and identify patterns that indicate breaches or attempted breaches with more agility and it supports more through auditory or cyber risks.

Organizations cannot rely on passive defense against cyber-attacks. Tapping into collective intelligence and joining automation to human intelligence can help organizations reduce risk of a cyber-attack and lower the costs of mitigation attacks.

Faced with these increasing information security threats, organizations have an urgent need to adopt IT governance best practice strategies. These strategies have benefits that add significant value to the organization by protecting the organization's reputation by creating sectors that have an urgent need to adopt IT governance best practice strategies.

4.0. OBSERVATIONS

It was observed that; -

1. Demand for cyber security specialist has become a more sellers' market as organizations and companies hurry to hire experts in the wake of several high profile cyber-attacks. It was therefore noted that shortage in specialized skills in cyber security and it has created gap in cyber security talent and it may not subside till year 2030.
2. Cyber threats have become too expensive to manage and cyber security management is a complex topic that requires substantial attention for it to be effective. This is not solely the responsibility of IT Department but working collaboratively across an organization.
3. Cyber security is becoming more frequent and costlier for businesses and organizations. Attackers are better funded and better organized than in the past and had led to dozens of banks have suffered cyber-attacks at the hands of foreign attackers.
4. Information sharing between private and public sectors is one of the collective means of fighting cyber -attacks or insecurity, it also reveals areas of investments and measures warranted to it.



5.0. RECOMMENDATIONS

The Delegation recommends that-

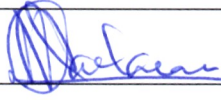
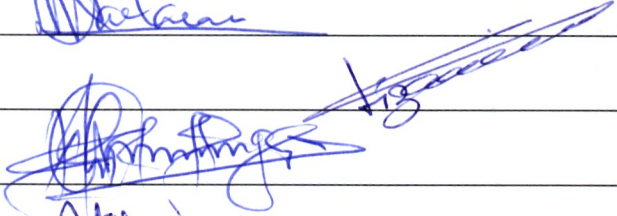
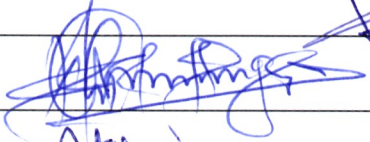
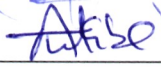
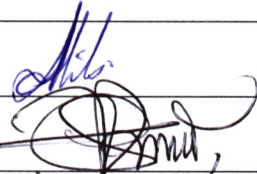

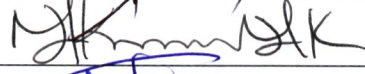
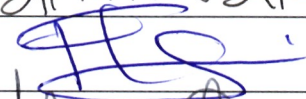
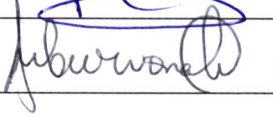

1. The Kenyan Parliament should consider allocating enough resources to Government sector's and cyber research institutes that implement the fight against cyber threats this is due to its complex nature and high cost of management.
2. Relevant Organizations should adopt an information security governance framework to embed cybersecurity into their corporate governance process.
3. Relevant State Department on matters education should consider tapping talent in schools and encouraging students to take up courses of ICT, as it is evident that there is shortage of experts in this field.
4. The Kenyan Government should endorse the information security governance framework and its core set of principles and encourage the private sector to make cybersecurity part of its corporate governance effort.

THE DEPARTMENTAL COMMITTEE ON COMMUNICATION, INFORMATION AND INNOVATION

MEMBERS ADOPTION LIST

Report on National Broadcasters Show held in Las Vegas, Nevada, USA from 7th -12th April

11th OCTOBER, 2018

NO.	NAME	SIGNATURE
1.	Hon. Kisang, William Kipkemoi, M.P - Chairperson	
	Hon.George, Macharia Kariuki, M.P - Vice – Chairperson	
3.	Hon.Liza, Chelule Chepkorir, M.P.	
4.	Hon.Alfah, O. Miruka, M.P.	
5.	Hon. Annie Wanjiku Kibeh, M.P.	
6.	Hon. Joshua Kimilu, Kivinda, M.P.	
7.	Hon.Marwa Kitayama Maisori, M.P.	
8.	Hon.Mwambu Mabongah, M.P.	
9.	Hon.Maritim Sylvanus, M.P.	
10.	Hon.Mwangaza Kawira, M.P.	
11.	Hon. Jonah Mburu, M.P.	
12.	Hon. Gertrude Mbeyu Mwanyanje, M.P	
13.	Hon.Wamuchomba, Gathoni, M.P.	
14.	Hon.(Eng).Mark Nyamita Ogola, M.P	
15.	Hon. John Kiarie Waweru, M.P.	
16.	Hon. Erastus Nzioka Kivasu, M.P.	
17.	Hon. Godfrey Osotsi, Atieno , M.P.	
18.	Hon. Innocent Momanyi, Obiri, M.P.	
19.	Hon.Anthony, Tom Oluoch, M.P.	

11
12
13



14
15

MINUTES OF THE 84TH SITTING OF THE DEPARTMENTAL COMMITTEE ON COMMUNICATION, INFORMATION AND INNOVATION HELD IN BOARDROOM ON 4TH FLOOR PROTECTION HOUSE, PARLIAMENT BUILDINGS ON THURSDAY 11TH OCTOBER, 2018 AT 10.00AM.

PRESENT

1. **Hon. William Kipkemoi, M.P.** -Chairperson
2. **Hon. George Macharia Kariuki, M.P.** -Vice- Chairperson
3. Hon. Annie Wanjiku Kibeh, M.P
4. Hon. Godfrey Osotsi Atieno, M.P
5. Hon. Maritim Sylvanus, MP
6. Hon. Mwangaza Kawira, M.P
7. Hon. Jonah Mburu, M.P.
8. Hon. John Kiarie Waweru, M.P
9. Hon. Liza Chelule Chepkorir ,M.P
10. Hon. Alfah O. Miruka, M.P
11. Hon. Erastus Nzioka Kivasu, M.P
12. Hon. Marwa Kitayama Maisori, M.P
1. Hon. Gertrude Mbeyu Mwanyanje, M.P

APOLOGIES

2. Hon. Mwambu Mabongah, M.P.
3. Hon. (Eng.). Mark Nyamita, M.P
4. Hon. Joshua Kimilu Kivinda, M.P.
5. Hon. Anthony Oluoch, M.P.
6. Hon. Wamuchomba Gathoni, M.P
7. Hon. Innocent Momanyi Obiri, M.P

IN ATTENDANCE

National Assembly Secretariat

1. Ella Kendi Clerk Assistant III
2. Ronald Walala Legal Counsel II
3. Elijah Ichwara Audio Officer
4. Mary Atieno Office Assistant

Consumer Federation of Kenya (COFEK)

1. Stephen Mutoro Secretary General

2. Benjamin Langat Vice Chairperson
3. Victor Gilo Programming Officer

MIN.NO./NA/CII/2018/310 PRELIMINARIES

The meeting was called to order at twenty minutes past ten o'clock followed with a word of prayer and introductions thereafter.

MIN.NO/NA/CII/2018/311: CONFIRMATION OF THE MINUTES OF THE PREVIOUS SITTING

The agenda was deferred to the next meeting.

MIN.NO/NA/CII/2018/312: MEETING WITH THE SECRETARY GENERAL, COFEK

The Secretary General submitted that;-

1. Cofek is Kenya's independent, self-funded, multi-sectoral, non political and apex non-profit federation committed to consumer protection.
2. Safaricom holds a higher percentage in the communications industry thus declaring it as dominant is not news and it should operate in a more restricted environment with controlled transparency, marketing and product pricing.
3. The potential overlap in powers between CA and CAK is a serious cause for concern as its not clear who between the two is legally most competent to determine, declare and impose conditions for dominance.
4. Competition Act needs to be amended to restrict it to over-arching competition policy and competition framework matters. The CAK have no monitoring tools, data and other legal sanctions as compared to the CA
5. The National Assembly CII committee has a locus standi on determining competition matters:
 - (i) It ought to demand answers on the process, schedules and intended consequences of their legislative powers from the CA.
 - (ii) It should be sucked into a fever pitch war between telecommunications firms
 - (iii) It is a state holder to the process, and cannot purport to influence and or direct the regulator which has independence under article 34 of the constitution
 - (iv) It needs to recuse itself and wait for the conclusion since it is carrying out a parallel process on a matter that has not been concluded by the sector regulator.
6. On matters concerning the market dominance, they were of the view that:

- (i) A person or entity that produces, supplies or otherwise controls not less than one-half of the total goods of any description that are produced , supplied or distributed in Kenya or any substantial part thereof or provides or otherwise controls not less than one half of the services rendered in Kenya or any substantial part thereof
- (ii) A market is therefore dominant when it holds a significant market power
- (iii) A market dominance in most jurisdictions is a market share of more than 50%
- (iv) Safaricom PLC is dominant and its competitors Airtel, Telkom Kenya and Faiba 4G are pale competitors. Thus calling safaricom as the dominant player is still not sure. This is because safaricom is in the same business as airtel and thus yes and no because they are not comparable in terms of market structure
- (v) That safaricom's competitiveness should be questioned. If its services provided if it's improving or declining or if safaricom is competing with itself.

7. On the issue of how dominance disrupts competitiveness, dominance affects competitiveness in the following ways;

- (i) Through promotions when a dominant operator give large discounts or promotions that the competitors can't be replicated,
- (ii) When a dominant operator puts concerted effort to ensure that a new competitor is not allowed to launch their services / delayed launch for the new competitor
- (iii) The fear of inability to enter the new market could be informed by insistence of the dominant player.

8. On the issue of dominance being decided on the basis of legal regulations or statistical assessment, it was noted that declaration of dominance is determined by both the statistical assessment and the legal regulations.

9. In order to protect the structure of measure, a grace period of at least 24 months should be given within which the negotiated interventions, pricing and promotion glide path should be undertaken with a view to establishing the best model of deterring potential abuse of the market leader and by equal measure developing targets and new SLAs which require that the minority competitors enhance their innovation, market access and investment in their respective models.

Committee Observations

1. The process of negotiated dominance means to progressively introduce remedies to address the anti-competitive behavior in the market. However, applying the process would take longer period to correct the imbalances in the telecommunication market.
2. COFEK was doing little to protect the interest of the consumers against exploitation by the operators in the market.
3. The public participation conducted by Communications Authority during drafting of the report on market study was not adequate and that there was need for a law that would enhance the thresh hold for public participation.

Committee resolutions

The Secretary General was directed submit a brief on;

1. Measures taken by other jurisdiction to protect the consumer in market where one operator controls the market.
2. Measures COFEK have taken to ensure that the consumers are protected against exploitation by the telecommunication operators in the market.

MIN.NO/NA/CII/2018/313 ADOPTION OF THE REPORTS ON FOREIGN TRAVEL

The Committee considered the following four reports on conferences attended by the Committee and adopted them as follows-

- (i) Report on Global System Mobile Association Mobile World Congress in Barcelona, Spain on 26th February to 1st March, 2018 was adopted having been proposed by Hon.George Kariuki MP and seconded by Hon.Annie Kibeh,MP
- (ii) Report on the invitation to Google Internet Academy in Wolmar, Mauritius on 7th to 9th March, 2018 was adopted having been proposed by Hon.Ersatus Kivasu,MP and seconded by Hon.Mwambu Mabongah,MP
- (iii)Report on 2nd Artificial Intelligence For Good Global Summit Held at ITU Headquarters in Geneva, Switzerland from 15th-17th May 2018 was adopted having been proposed by Hon.Liza Chelule,MP and seconded by Hon.Alfa Miruka,MP
- (iv)Report on National Broadcasters Show held in Las Vegas, Nevada, USA from 7th - 12th April was adopted having been proposed by Hon.Jonah Mburu,MP and seconded by Hon. William Kisang,MP

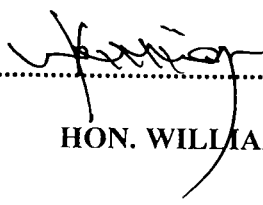
It was resolved to adopt the following two reports during the next meeting:-

- (i) International Broadcasting Convention Conference held in RAI Amstredam, Netherlands on 13th to 17th September, 2018
- (ii) World Summit on the Information Society (WSIS) Forum held in Geneva, Switzerland on 19th to 23rd March, 2018

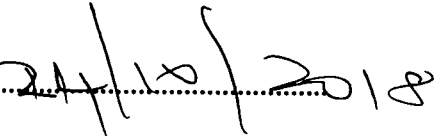
MIN.NO/NA/CII/2018/314 ADJOURNMENT

There being no other business, the meeting was adjourned at thirty minutes past twelve o'clock.

SIGNED.....



DATE.....



HON. WILLIAM KISANG, MP- CHAIRPERSON

1
2
3
4

1
2
3
4

00

1
2
3