REPORT OF THE PUBLIC INQUIRY ON THE LAWFUL INTERCEPTION OF COMMUNICATIONS REGULATIONS

1.0. INTRODUCTION

The Nigerian Communications Commission (the Commission) pursuant to its powers under Section 70 of the Nigerian Communications Act 2003 (the Act) developed the draft Lawful Interception of Communications Regulations (the Regulations). Based on the Commission's policy of participatory rule-making, the Regulations was published on its website for Comment from the general public, especially telecommunications operators and other stakeholders.

Further to this, the Commission received Five (5) submissions from the following stakeholders:

1. Airtel Networks Limited
2. Emerging Markets Telecommunication Services Limited (trading as Etisalat)
3. MTN Nigeria Communications Limited
4. National Human Rights Commission; and
5. Mr. Christian Oronsaye.

As required by law, a public Inquiry on the Regulations was scheduled for July 7, 2015 and a Notice of the Public Inquiry was published in Guardian Newspapers on Wednesday June 24, 2015, in This Day Newspapers on Thursday June 25, 2015 as well as in Vanguard Newspapers on Tuesday June 30, 2015.

2.0. THE PUBLIC INQUIRY

The Inquiry held as scheduled at the Conference Hall of the Commission. The forum commenced at 11:30am and was chaired by the Executive Vice Chairman, represented by the Executive Commissioner, Stakeholders Management, Dr. Okechukwu Itanyi. Staff of the Commission and over Seventy Three (73) persons made up of representatives of telecommunications companies, interested stakeholders and the media attended the forum.

The EC(SM) welcomed participants to the forum. He explained that the Inquiry was part of the rule-making process adopted by the Commission to ensure wide consultations in the making of regulations by the Commission. He highlighted the primary objectives of the Regulations which include:

- Providing the legal and regulatory framework for the lawful interception of communications, collection and disclosure of intercepted communications in Nigeria.
- Ensuring respect for privacy of subscribers' communications as preserved under the Constitution.
- Specifying the type of communications that can be intercepted and prescribing the penalties for non-compliance with the Regulations.

The EC(SM) enjoined all participants to freely make their contributions and raise issues that would assist the Commission in coming up with regulations that would enhance development of the industry and the entire economy.

The Head, Legal & Regulatory Services, Mrs. Yetunde Akinloye gave a short overview of the Regulations. This was followed by a presentation by Mr. Gwa Tobbie Mohammed (Assistant Director, Legal & Regulatory Services) on issues raised on the Regulations prior to the Public Inquiry.

A. General Overview of the Licensing Regulations

The draft Regulations is made up of Twenty Four (24) Regulations and structured into Seven (7) Parts. The Regulations deal with several issues including the Scope and Objective of the Regulations, Interception of Communications, Administration of Lawful Interception of Communications, Interception Capabilities as well as rules relating to Protected or Encrypted Communications.

B. Review of Submissions Received

The Commission had prior to the Public Inquiry reviewed the submissions received from stakeholders and its response to the issues raised are set out below.

1. Objectives

Comment

The objectives do not provide for the rights and protections available to service providers. The Regulations should indicate that Licensees are protected pursuant to Section 146(3) of the Act where they have complied with the provisions of these Regulations.

Response

Regulation 1(a) already makes reference to Section 146 of the Act. Moreover, Regulation 6 has provided further safeguards for operators.

2. **Preservation of the privacy of subscribers as contained in the Constitution**

Comment
The Regulations refers to "privacy of subscribers", but does not state how this can be achieved.

Response
Reference in the Regulations to "privacy of subscribers" was in error. This will be redrafted to now read "privacy of subscribers' communications"

3. **Application - These Regulations shall be in operation in the Federal Republic of Nigeria**

Comment
Clarification is sought on whether outbound roaming services will be subject to the Regulations.

Response
The Regulations shall apply to communications emanating from the operators network including outbound roaming services on the basis that they emanate from Nigeria. Regulation 6(1)(b) deals with this issue and it is explicit.

4. **Unlawful Interception of Communications**

Comment
The penalty for breach of Regulation 3 is not clearly stated.

Response
Noted. The penalty for unlawful interception will be provided under Regulation 20.

Regulation 20 will be amended to state that *"Any person or Licensee that fails to comply with the provisions of these Regulations shall be liable to a fine of ₦5,000,000.00. If such an offence is continuing, such a person or Licensee shall be liable to a daily default penalty of ₦500,000.00."*

5. **Interception without a Warrant**

Comment 1
Regulation 4(1) (a) is sufficient, and (b) is redundant and repetitive.

Response
Noted. Regulation 4(1)(b) will be deleted.

Comment 2
Regulation 4(1) is a departure from the rationale behind Section 146 and 147 (national interest matters) of the Act. Interception of communications should not be done for private purposes.

Response
The safety of every Nigerian citizen should be of national interest. This therefore supports the interception of communications of a private person.

6. Interception without a Warrant

Comment 1
The categories under Regulation 4(2)(a) may be mutually exclusive and should be redrafted.

Response
Accepted. This proviso will be redrafted as follows: "… *if done by a person who is a party to a Communication, provided such a person has sufficient reason to believe that there is a threat to human life and safety* ***OR*** *who in the ordinary course of business is required to record or monitor Communication"*

Comment 2
Regulation 4(2) should be expunged because it is incompatible with Section 37 of the 1999 Constitution.

Response
Regulation 4(2) has been redrafted.

Comment 3
Regulation 4(2)(b) is unclear and gives the impression that service providers currently intercept and/or archive communications content in the ordinary course of their business. This goes against the general purpose of Section 146 of the Act. Regulations should focus on interception of communications as contemplated in Section 146 of Act.

Response
Regulation 4(2)(b) will be deleted.

7. Interception with a Warrant

Comment
The phrase *"the interception of any communication as described in the Warrant"* in Regulation 5(1) is hanging and should be properly inserted into the relevant provision.

Response
Accepted. This will be inserted and renumbered accordingly.

8. Grounds on which a Judge is permitted to issue a Warrant

Comment
The application for the warrant should include a declaration by the requesting authority that there is no other lawful means of investigating the matter for which the warrant is required. This is necessary to prevent abuse.

Response
Regulations 5(2)(b) and 7(3)(f) state that a warrant may be applied for where there is no other lawful means of investigating the matter.

This provision has however been redrafted to include a requirement for deposing to an affidavit on Oath stating that there is no such other means.

9. Justifications for interception

Comment 1
The provision should clearly prohibit usage of intercepted information for any purpose outside of those listed. Such unsanctioned usage should be criminalized and attended with appropriate penalties.

Response
The warrant as noted from the provisions of Regulation 5(3) is issued for the purpose set out in 5(3)(a) - (e) and subject to the express consent of the relevant judge as set out in Regulation 14. Regulation 19(3) also provides for usage.

Comment 2
These justifications should be clearly stated at the beginning of the draft and should be reviewed to include *the prevention of injury to or trafficking in vulnerable persons such as children, women, persons with disabilities as well as prevention of corruption and laundering of money associated to these.*

Response
Regulation 5(3)(b) adequately covers this.

10. Interception with a Warrant

Comment
Regulation 5 (3) (c) should be expunged as it may provide grounds for abuse by Law Enforcement Agencies (LEAs). Regulation 5(3)(d) that provides the necessity of a warrant in the interest of public emergency or public safety, will suffice in this regard.

Response
Not accepted. Economic well-being and public emergency/safety issues dealt with under the (c) and (d) are different.

11. Power to Lawfully Intercept Communication

Comment 1
The protection under Regulation 6(1) should also include civil liabilities.

Response
Accepted. This will be redrafted to include civil liabilities. Indemnity options will also be explored.

Comment 2
Given the potentially high level of liabilities, such a protection offered by the proviso in Regulation 6 should be backed by legislation. This protection should not be placed in a proviso as its impact may be whittled or constricted to the situations covered by this paragraph.

Response
This provision is sufficient as a proviso.

12. Application for a warrant

Comment 1
Regulation 7 should define a designee and clearly provide for how the designate of the National Security Adviser (NSA) and the Director of the State Security Service (SSS) will be appointed.

Response
There is no need for definition. The Regulations cannot determine how an organisation appoints its designee as these are operational issues.

Comment 2

The police, NDLEA, ICPC, EFCC, etc should be included among those under Regulation 7(1) who can apply for warrants for law enforcement purposes under adequate safeguards.

Response

Accepted. However, this will be redrafted to include only the Police in view of its mandate to prevent and detect crime under the Police Act.

Comment 3

The NSA and SSS do not have operational responsibilities. Centralizing these roles in the above agencies makes the proposed regime potentially counter-productive.

Response

These agencies have been empowered to handle the sensitive information and provide the evidence if necessary to the other LEAs. This supports the protection of the privacy of Nigerians. Allowing other Agencies might open lawful interception to abuse which may be difficult to trace.

13. Contents of Supporting Material for an Application for a Warrant

Comment

Information in support of an application for interception should be provided in an affidavit or under oath to ensure that there is a threat of legal consequences for not being truthful in this manner.

Response

Noted. Regulation 7(3) will be redrafted to include a supporting affidavit for an application for a warrant.

14. Requirement for application for warrant to state the location where Lawful Interception will take place

Comment

This should be deleted as Lawful Interception (LI) is not a location dependent service.

Response
Accepted. The suggested amendment to Regulation 7(3) (e) will be considered.

15. Power of the NSA to initiate and request from the Licensees, interception of Communications without warrant in cases of emergency

Comment 1
Regulation 7(4) has the potential to expose operators to civil suits for which the draft does not protect operators against and should be promulgated as legislation to offer protection to operators.

Response
Operators will not be able to intercept communications. The Authorised Agencies may intercept without the knowledge of operators. This provision is therefore no longer relevant.

Comment 2
Duration should be reduced from 48 hours to 24 hours. This will prevent abuse of the process. The proposed 48 hours window may be sufficient for the LEA to gather whatsoever data that is required before the warrant is rejected.

Response
There may be times such as the weekend where it is impossible to get a warrant.

Comment 3
The term "Emergency" should be defined to ensure that there is no abuse of the LI process when intercepting without a warrant.

Response
Emergency will be based on the interpretation and evaluation of the circumstances at the time of making a determination to intercept by the NSA, SSS or Police.

Comment 4
The Office of the NSA should be under obligation to make a formal report of cases in which emergency interception has been effected at the end of each year.

Response

The Regulations will be redrafted to provide for a log book to be kept by the NSA for yearly review by the Attorney General. However, this will be in respect of concluded cases, as secrecy may still be required for ongoing matters.

16. Issue and Content of a Warrant

Comment

Installation of any equipment for the interception of communications or the operations of LI equipment should take into account the impact on the network's ability to fulfil its primary objective to provide services to consumers and preserve network integrity and interoperability.

Response

Regulation 8(2)(a) will be redrafted to state that the equipment to be installed for lawful intercept shall comply with the Commission's technical requirements such as type-approval for network components, and shall not be such as to negatively affect the operations of the licensee in terms of its capability to provide uninterrupted network services.

17. The Warrant may authorize the relevant LEA to return any Communication that was taken into possession or cause it to be returned to the Licensee

Comment

Further to Regulation 8(2)(c), there should be a proviso clearly voiding and rendering inadmissible such acquired information if the requesting warrant is rejected. This will also serve as a check against abuse of the LI process and encourage adherence to the Regulations.

Response

This will be applicable in circumstances where interception is without warrant. Proviso will be inserted under Regulation 8 stating that any information obtained where an application for warrant is refused will be invalid.

18. A Judge may only issue a Warrant if satisfied of certain conditions

Comment

There should also be an inclusion in Regulation 8(3) of an affidavit on oath to justify the belief that the matter in question can only be investigated through interception.

Response
Accepted. See the Commission's comments in Regulation 7(3).

19. The Commission shall be notified in writing by the Licensee of all Warrants presented to it, notification to the Commission shall be no later than 48 hours after receipt of the Warrant by the Licensee

Comment 1
This should be expunged. Based on Regulation 5(3), interception is only allowed in matters where utmost secrecy and confidentiality is required at all times.

Response
This provision will be deleted not for the reason advanced but because licensees are not expected to intercept communications.

Comment 2
The NSA should be required to keep a comprehensive log which would be presented before the Chief Judge of the Federal High Court or the Attorney-General of the Federation for review at the end.

Response
The Regulations will be redrafted to provide for a log book to be kept by the NSA for yearly review by the Attorney General.

20. Duration, Amendment, Cancellation and Renewal of Warrant

Comment
A warrant should only be varied, amended, extended or cancelled by the same judge who issued it except where it is impossible to do so. This will prevent abuse of court processes which may occur when a dissatisfied applicant chooses to go before another judge in search of more lenient treatment.

Response

Noted. This provision will be included in the Regulations. There will however be an exception to this provision where it is impossible to do so by reason of the death, incapacity or other unavailability of the said Judge.

21. Implementation of a warrant to be effected by NSA and SSS only

Comment

Regulation 10(1) does not specify the role of the Nigerian Police Force and other agencies. Even though Regulation 23 makes reference to LEA which is defined to include the Police among other agencies.

Response

We shall correct the omission and align it with relevant authorities as defined under the Enforcement Processes Regulations. However, only the NSA, SSS and the Police will have the powers under these Regulations to carry out interception of communications.

22. The implementation of such Warrant may if required by the NSA or SSS take place with the collaboration of the Licensees

Comment

Clarification is required on Regulation 10(2) particularly in view of deliberations on automated processes that have taken place to date with the Office of the NSA.

Response

This provision addresses circumstances where it may be necessary for the NSA to seek collaboration with the operator notwithstanding the automated process in place.

23. Disclosure of intercepted material obtained or provision of related communication data to the LEA

Comment

The phrase "related communication data" should be defined.

Response
Noted. Definition will be provided.

24. Licensees expected to take such steps as the NCC may by way of notice direct to install interception capabilities

Comment 1
Further to Regulation 12(2), there should be a final cut-off date, after which any further upgrade will cease to be at the expense of the operators, as is obtainable in other jurisdictions.

Response
Not accepted. Section 147 of the Act which confers power on the Commission to determine technical specifications for LI does not admit any limitations as to time. Regulation 11 & 12 are in conformity with Section 147.

Comment 2
It was also suggested that the specification of equipment to be used in the LI process be scalable and operators be granted import duty waiver for the equipment and other appropriate concessions for the LI process.

Response
The Commission cannot request for a duty waiver on LI equipment as operators in accordance with the Act are expected to make their systems LI compliant.

25. Interception capability: Commission to provide specifications and technical requirement of LI equipment provided by the Commission from time to time

Comment
Service providers should be fully involved in developing any technical requirements of equipment before mandating any amendment under Regulation 11(3) to the currently prescribed capabilities. In this regard, the potential impact on service delivery should be critically assessed when requesting for equipment to be installed for interception of communications.

Response

The Commission in developing rules and regulations always embarks on wide consultation with the industry. However, a change or upgrade in the technical specifications may be requested by the NSA and operators will be obliged to comply. This is inevitable due to the nature of technology which keeps evolving. The Regulations will be redrafted to reflect this.

26. **The Licensee shall remain compliant with the provisions of this Regulation and ensure that its system updates and upgrades do not adversely impact the implementation of this Regulation**

Comment

Regulation 11(5) should take into account force majeure, infrastructure disruptions and other unforeseen events which may result in technical issues that impact intercept activities.

Response

The provision will be redrafted to exclude cases of Force Majeure.

27. **Acquisition of necessary facilities and devices by Licensees to enable the monitoring of Communications**

Comment

International best practice indicates that neither the service provider nor the government bears the entire burden of costs for the implementation of LI; rather, parties all assume responsibility for those costs which they would reasonably be expected to bear in the performance of their obligations under the initiative.

Response

The operators are only bearing their respective costs which is consistent with international best practice. Regulation 12(2) is consistent with Section 146 (2) of the Act.

28. **Burden by Licensee to bear investment, technical, maintenance and operating costs**

Comment

Regulation 12(3) should be amended to highlight the fact that Operators will only be responsible for any financial obligations of ensuring that intercept capabilities are installed on their own facilities.

Response
This provision is clear enough.

29. Disclosure of Protected or Encrypted Communication

Comment 1
Under Regulation 13, orders involving interception or compulsion of hand-over of encryption keys should be directed to the subscribers or direct holders of the encryption keys instead of the Licensees or service providers.

Response
The Regulations will be redrafted to compel the person in possession of the key or code to provide it to the Authorised Agency upon request.

Comment 2
This provision is not capable of being implemented as several value added services provided by non-licensed entities such as Blackberry services by RIM, Facetime service by Apple Inc., other services provided by Google, etc. (generally known as "Over-the-top"/(OTT) utilize encrypted formats which cannot be accessed by operators. Operators are neither permitted by law, nor technically capable to have visibility of such communication.

Response
The Regulations have been redrafted to enable the Authorised Agency seek foreign mutual assistance to obtain a key or code.

Comment 3
This should be amended to require the person who has the code to disclose it in accordance with the warrants.

Response
Regulation 13(2) recognizes that the key or code may be in the possession of another person. In which case the obligation of the licensee is to request such person to disclose the key/code.

Comment 4

Orders involving interception or compulsion of hand-over of encryption keys should be directed at the subscribers or direct holders of encryption keys instead of the Licensees or service providers.

Response
Regulation 13(3) deals with scenarios of how the provision of the Regulation may be satisfied where the communication is encrypted or protected.

For clarity, Regulations 13(3)(a) & (b) have been redrafted as follows:

(a) *The Licensee or any person affected by Regulation 13(2) has provided or disclosed key, code, access to the protected, encrypted Communications to the law enforcement agent; or*

(b) *The Licensee or any person affected by Regulation 13(2) in possession of the key or code has made a disclosure of any protected or encrypted communication in an intelligible form.*

30. Use of Information Obtained under these Regulations

Comment
The primary test of admissibility is relevance, and at all times, it is the discretion of the trial judge what evidence to admit or reject, subject to the right of either party to appeal such decision. Regulation 14 may therefore amount to an attempt to inadvertently amend the provisions of the Evidence Act. Therefore, the Commission is requested to kindly reconsider its inclusion.

Response
The Regulation does not seek to amend the provisions of the Evidence Act in relation to admissibility of evidence. Moreover, the use of such information is also made subject to the discretion of the judge.

31. Secrecy

Comment 1
Regulation 15 should be broadened to require that a warrant be issued for any subsequent disclosure of information sourced from session(s) of interception of Communication for which the initial warrant did not provide for.

Response
Any further interception in connection with another session of the same communication would require another warrant where the new session is outside the scope of the existing warrant. This is because a warrant indicates a detailed description of the communication to be intercepted, and also has duration. See Regulation 8(1)(c) & (e).

Comment 2
In order to ensure that only authorised persons are allowed access to intercepted communication, the consent/approval of a security officer not below the rank of Assistant Commissioner of Police (or equivalent rank) and the written consent of the NSA or SSS should be required for the release of this information.

Response
The Regulations shall be redrafted to indicate the suggested provision in accordance with the Enforcement Regulations.

Comment 3
The LEAs and others mentioned in this Regulation are ordinarily not subject to the regulation of the Commission. It is very doubtful if such provisions can be enforced against such persons, particularly if their actions lead to losses or other impairment to licensees. It is therefore recommended that the provisions herein be included in an enabling Act of the National Assembly along with the indemnity provisions in 6(1) above.

Response
The inclusion of the provision in this Regulation bears as much weight in law as if it were in an Act of the National Assembly. The position of the law is that a subsidiary legislation has the force of law. This position implies that regulations, rules, bye-laws made pursuant to an act/law will qualify as a subsidiary legislation.

It must however be noted that the enforcement of these provisions do not necessarily have to be by the Commission as an aggrieved person can approach the courts for redress.

32. Requirement to Maintain Logbook of all Warrants

Comment 1
Regulation 16 is vague and there is a need to clearly specify persons entitled to view the Log book.

Response
The Regulations will be more specific i.e. permitting only LEA to view log book or such other person that may have a court order to view same.

Comment 2
The Log book should be open for public inspection under clearly stated conditions.

Response
The Log book cannot be made open for public inspection for security reasons.

Comment 3
In line with international best practice and given that the Commission is not primarily involved with interception and other activities pertaining to it, the obligation of keeping a log should be the responsibility of the parties listed in Regulation 7 above.

Response
The Regulations will provide that the NSA, SSS and Police should keep log books of interceptions made. These books should be presented to the Attorney General at the end of the year.

Comment 4
Regulation 16(3) requires the Commission to prepare a report and should require the Commission to publish its annual report on interceptions, submit the report to the National Assembly and ensure public access to the report.

Response
The reason behind the obligation to prepare a report is for record purposes, it is confidential and not for dissemination to the public. It is therefore not advisable to permit easy public access of such information.

Comment 5
An application for interception should be notified to the Commission and any warrant issued under this should also be notified within a stipulated time limit.

Response
Not accepted. The Authorised Agencies will keep a logbook of all intercepted communication.

33. Judicial Review

Comment 1
Regulation 17 should stipulate under what conditions and within what time limits interception subjects should be notified of interception process against them.

Response
Placing the interception subject on notice is counterproductive and defeats the very essence of intelligence/ information gathering.

Comment 2
There is no general affirmation of the entitlement of subscribers to privacy of their communications. There are also no provisions for the rights of private citizens to a cause of action where there is an alleged breach and abuse of the process for the interception.

Response
The intercepted subject becomes aware in cases where based on intelligence/information gathered an arrest is made and during the course of trial such intercepted subject is found to have been wrongfully arrested. Hence the remedy for judicial review.

Comment 3
The draft Regulations should include a specific acknowledgement of the constitutional right to privacy of subscribers and the obligation of regulators, licensees and law enforcement agencies to respect this right except in accordance with the allowance provided under Section 45 of the Constitution.

Response
The Regulations categorically provide that it is illegal to intercept communications except as provided in the Regulations. This is to ensure the privacy of communications of subscribers. The constitutional value is therefore preserved as it is only under the exceptions set out in the Regulations that interception is permissible.

The right of an individual to litigate or protect his/her right is guaranteed by the Constitution and we believe that the regulation is not a clog in the exercise of that right. The award of damages or other awards are solely within the discretionary powers of Courts which are enabled to make such determination.

Comment 4
This Regulation does not consider circumstances in which any interception of communication in itself may lead to a severe adverse impact on network operations, a subsequent inability of the network to offer services to customers/ emergency services and a potential threat to lives.

Response
There is no need to for this. Interception of Communication will not impact negatively on any licensee's network as long as the licensee meets the technical specifications agreed upon.

Comment 5
It is recommended that the merits of any complaints by an aggrieved party involved in any interception of communication be initially considered by an arbitrator. The arbitrator should be provided with the powers to decide, based on the merits of the complaint, whether to place on hold the decision to intercept communication pending the results of a final review of the complaint by a court.

Response

It is also unlikely that a subscriber will be aware of any interception being made until the conclusion of such investigation. This also pertains to criminal activity which is beyond the powers of an arbitrator.

Comment 6
It is not clear which court is referred to in this provision.

Response
The constitutional jurisdiction of such matters resides in the Federal High Court. The court would however be specified for clarity.

Comment 7
Under Regulation 17(2), a Warrant should only be varied, amended, extended or cancelled by the same judge that issued the Warrant, except where it is impossible to do so by reason of the death, incapacity or other permanent unavailability of the said Judge.

Response
Noted. This has been addressed under remarks on Regulation 9.

34. Storage of archived Communications – Such communication to be stored on the communication system of a licensee for a period of 3 years

Comment
Regulation 18 should be modified to reflect that the state will bear the cost of any additional logistics/storage capacity that may be required to store any intercepted communication for the period.

Response
Not accepted. Operators must ensure that they install such capabilities that enable the operator to store archived communications. The cost of this will be borne by the operator.

35. Storage of Intercepted Material

Comment
Regulation 19 does not incorporate any measures to compel/confirm the destruction of intercepted material once its purpose has been fulfilled.

Response
The Regulations state that the communication shall be destroyed upon completion of such investigation. The use of the word 'shall' in this context makes destruction of the intercepted communication mandatory.

36. Redaction of Non-Useful Information/Data Intercepted

Comment
A procedure for redaction must be set out in the Regulations. This will assure the citizens of privacy protection and also limit the use of such non-relevant information for non-authorised purposes.

Response
Regulation 19 will be widened to deal with unused communications in specific instances.

37. Storage of Intercepted Material

Comment
Retention period should be included under Regulation 19 (1). Suggestion of no more than 6 months in any case and in the event that there is a need to exceed this term, an application should be made to the Federal High Court for such purpose.

Response
Noted. The Clause will be redrafted to provide for the data to be archived for 3 years and thereafter destroyed.

38. Penalties for Contravention – Revocation of Licence

Comment 1
Regulation 20(b) would appear to contradict the clear provisions of Section 45(2) of the Act as well as the provisions of the respective licenses on the process for licence revocation.

Response
Noted. The Commission will redraft the Regulation and revocation will be in accordance with Section 45(2) of the Act.

Comment 2
It was observed that while penalties are provided for operators, none is provided for law enforcement agencies and other parties who deal with intercepted communications

Response
LEAs are not within the regulatory control of the Commission. It will not serve any purpose to provide such penalties against LEAs. Suffice to say that the courts have

powers to entertain any person who has a grievance against LEAs for any breach of rights under the Regulations.

39. General Interpretation

Comment 1
The term "NSA" is only used in this regulation and no other provision has this abbreviation. This should be deleted.

Response
Noted.

Comment 2
A definition be included for "designee".

Response
The term is of common usage hence there is no need for a specific definition.

40. Nature of Legal Instrument Required

Comment
The text and structure of the Constitution suggest quite strongly that the kind of limitations proposed by these Regulations should be achieved not by subsidiary legislation but by primary legislation.

Response
The position of the law is that a subsidiary legislation has the force of law. Moreover, the regulations only provide details in respect of the express provisions of Section 147 of the Act and the Wireless Telegraphy Act.

41. Typographical Errors

Comment 1
The draft Regulations should be subjected to further editing in order to remedy typographical errors and other errors evident in the text of the Regulations.

Response
Noted.

Comment 2
Under Regulation 1(e), the spelling of 'persevered' should be corrected to 'preserved'.

Response

Noted.

Comment 3
Under Regulation 7(3)(f), the following was omitted "state that.."

Response
Noted.

Comment 3
Under Regulation 13(3)(a)(b), the word "person" should be placed after "any" for the sentences to flow.

Response
Noted.

42. Justification for Interception Regime as an invasion of constitutionally protected right

Comment
The only justification for the regime of interceptions that the Regulations seek to create are a narrowly constructed national security or defence justification.

Response
The Regulations are drafted in line with the exception under Section 45 of the constitution. Justification for this is also provided by the Wireless Telegraphy Act.

43. Inclusion of an intermediary for the execution of Lawful Interception Warrants

Comment 1
Issuing a warrant to an operator for the purposes of 'providing assistance' for LI serves no purpose as Operators have no visibility into what communication is being intercepted or when it is being intercepted.

Response
Accepted. The Regulations will be redrafted.

Comment 2
Due to the sensitive nature of LI, a suggestion was made for an Ombudsman, an independent body or person, whose sole and primary duty would be to ensure that there is no abuse of the LI process. The office should be empowered by law to serve as a watchdog as obtains in other jurisdictions.

Response

Checks and balances are provided through the judicial process. Interception with warrants follows a process, whilst interception without warrants is also required to follow a process.

The essence of stipulating the warrant application process is also to provide a regulatory framework for interception in order to eliminate the abuse traditionally associated with LI.

C. Additional Issues Raised at the Public Inquiry

At the Public Inquiry, stakeholders made comments and raised additional issues which the Commission addressed. Highlights of the issues that were raised and response given by the Commission are as follows:

1. Interception of Communications

Comment

The Regulations should include provisions requiring LEAs to obtain the consent of telecommunications operators before an interception of communication can be effected. This is because the contract a subscriber has is with the Telecoms Operators.

Response

The Regulations has put in place the requirement to obtain a warrant from a judge before an interception can be carried out. This is to ensure that the power to intercept communications conferred on LEAs is not abused.

2. Powers of the Attorney General of the Federation

Comment

Under the Regulations, the activities of LEAs regarding LI are supposed to be checked by the Attorney General of the Federation (AGF) through the annual audit. However, the fact that the AGF is a political appointee brings into question the issue of accountability.

Response

Though the AGF is a political appointee, the Regulations have in place checks and balances to ensure that no provision of the Regulations is abused. In view of this, there is the provision of judicial review for any person aggrieved under the Regulations to approach a court of law for review of such matter.

3. Protected or Encrypted Communications

Comment

The blanket requirement that operators should give access to encryption keys as provided under the Regulations should be reviewed.

Response
There is adequate provisions in the Regulations to ensure that the key or code to any encrypted communication that has been intercepted is only provided to LEAs upon request by the person in possession of such key or code.

4. Judicial Review

Comment
Recourse to the court of law should be allowed under the Regulations where an aggrieved person believes that his communications have been misused.

Response
The Regulations do not prohibit any person aggrieved by any interception activity to seek judicial review.

5. Protection of Subscribers' Privacy

Comment
The provisions of the Constitution which guarantees the privacy of telephone conversations and telegraphic communications of every citizen cannot be altered by way of a Regulations. It is therefore recommended that the Commission should consider either amending the Act in order to reflect the changes proposed under the Regulations or follow up at the National Assembly to ensure that the Lawful Interception of Communications Bill is passed into law.

Response
The Regulations do not in any way alter the provisions of the Constitution. It spells out the procedure by which LEAs can intercept communications within the ambit of the law, without derogating from the right to privacy of citizens as guaranteed under the Constitution. This is why in drafting the Regulations, the Commission has put in place checks and balances e.g. interception with warrant, judicial review, keeping of logbooks etc.

6. Powers of the Commission to make Rules on Interception of Communications

Comment
Section 38 of the recently passed Cybercrimes (Prohibition, Prevention, Etc.) Act 2015 specifically provides for lawful interception of communications. It also spells out the responsibilities of the AGF, Office of the NSA and the Commission. Under the Cybercrimes Act, the Commission is only given the power to prescribe what constitutes traffic data and subscriber information for the purpose of record retention while the AGF has the power to make regulations under the Cybercrimes Act.

It therefore means that the Commission cannot ascribe any other functions to itself with regards to lawful interception of communications since the Cybercrimes Act is later in time and takes precedence over the Act.

Response
The Cybercrimes Act does not amend or repeal any provision of the Act. The Act and the Wireless Telegraphy Act (WTA) specifies that any issue of interception of communications is the responsibility of the Commission. Based on the powers already conferred on the Commission by the Act and the WTA, the Regulations seeks to spell out procedural issues not covered under the Act and WTA. The Act and the WTA therefore remain subsisting laws until amended or repealed by the National Assembly.

7. Conflict between the Regulations and Freedom of Information Act

Comment
The Commission should take into consideration the provisions of the Freedom of Information (FOI) Act regarding the restriction on disclosure of information. This is because where there is a conflict between the Regulations and FOI Act, the provisions of the FOI Act will prevail.

Response
The provisions of the FOI Act deals with disclosure of information in the custody of public institutions. It therefore means that the FOI Act would have no impact on interception of communications which is on information in the custody of Telecoms Operators.

8. Cost of Purchasing and Installing Equipment that have Interception Capabilities

Comment
The cost of purchasing and installing equipment that have lawful interception capabilities should be deducted from the Annual Operating Levy payable by Operators in order to lessen the cost-related burden imposed on Operators under the Regulations.

Response
The Act has already specifically placed an obligation on all Operators to ensure that their equipment and systems have intercept capabilities in line with international best practices. This is not a new obligation hence the Operators will have to bear the cost of purchasing and installing such equipment.

3.0. GENERAL COMMENTS

The Head, Legal and Regulatory Services thanked everyone for coming and assured them that all comments will be considered by the Commission before the Regulations are finalized.

The Public Inquiry ended at 12:40pm.

Dated this 7th day of July 2015

Dr. Eugene I. Juwah
Executive Vice-Chairman/CEO
NIGERIAN COMMUNICATIONS COMMISSION