REPUBLIC OF IRAQ

COMMUNICATIONS AND MEDIA COMMISSION

CONSULTATION DOCUMENT

REGULATION ON ASSISTANCE FOR LAWFUL INTERCEPTION AND DATA RETENTION

JUNE 2016

1. INTRODUCTION

Pursuant to the Constitution and Coalition Provisional Authority Order 65 (Order 65), the Communications and Media Commission (the Commission) is empowered to regulate telecommunications and information services sector in the Republic of Iraq.

The Commission has engaged a firm of consultants to assist it with a review of the existing regulatory framework. Having carried out this review in regard to the legal powers and mandates of the Commission, the status, need for, and international best practices on Legal Interception and Data Retention regulation, the consultants have produced a draft Regulation governing Legal Interception and Data Retention, which has been considered and endorsed by the Commission.

Now the Commission wishes to obtain the views of interested individuals and persons on this proposed regulation, which conforms to international best practice and the relevant laws of the Republic of Iraq, before the Commission considers these for their final approval and implementation.

Hence, the Commission invites the public, telecommunications and information services sector licensees and other interested persons to provide it with their comments on the information set out in this document. Any views or comments should be made in writing addressed to:

IRAQ – Baghdad

Al masbah – hay babel

District #: 929, Street #: 32, Building #: 18

Or electronically to;

consultation@cmc.iq

22/7/2016

Submissions are needed in soft copy only and may be in English or Arabic; dual-language submissions will be extremely helpful.

In the interests of transparency, the Commission expects to publish submissions. Stakeholders should indicate clearly any part of their submission that they would not wish to be included in a published version, explaining why such part should be treated as confidential.

REGULATION ON ASSISTANCE FORLAWFUL INTERCEPTION AND DATA RETENTION

PREAMBLE

On this __ day of __, 2016, the Board of the Communications and Media Commission of Iraq hereby issues the following Regulation:

AUTHORITY

The Commission, aftercareful consideration of the provisions of the Constitution of Iraq, including Article 40 providing that "[t]he freedom of communication, and mail, telegraphic, electronic and telephonic correspondence, and other correspondence shall be guaranteed and may not be monitored, wiretapped or disclosed except for legal and security necessity and by a judicial decision," read in conjunction with Article 2C that "[n]o law that contradicts the rights and basic freedoms stipulated in this constitution may be established;" as well as taking note of the authority granted by the Constitution's Article 130 in conjunction with Articles 103 and 110 for the Communications and Media Commissionto regulate telecommunications policy on behalf of the federal government as an independent institution under the law; and with reference to the Coalition Provisional Authority Order 65, providing in Article 1.5 thereof for the Commission to ensure that Iraqi telecommunications are operated in a manner consistent with public safety, and in keeping with the comity provisions of Article 5 of said Order, as well as the powers enumerated in Articles 3 and 4 thereof, has decided as follows:

RECITATIONS

Mindful of the difficult security situation the country is experiencing and the importance of preventing Telecommunications and Information Services frombeing abused for illegal aims undermining the security of the country;

Aware of the urgent need of the security forces to be provided with assistance by Telecommunications and Information Services Providers appropriate to facilitate law enforcement for the benefit of society; and

Cognizant of the need to balance competing fundamental rights to privacy and security in an appropriate manner,

have determined to promulgate the following regulation:

Article I. Scope and Objectives

This regulation promulgated by the Commission obliges all Providers of jurisdictional Telecommunications and Information Services to establish and maintain capabilities for lawful interception as well as the retention of certain data, and to provide implementation mechanisms therefore.

Article II. Definitions

For purposes of this regulation, the following terms shall have the specified meaning:

(1) *Appropriate Judicial Authorization* means for purposes of this regulation an authorization, issued by a court of competent jurisdiction, to intercept and/or access Content, Traffic Data or both, relating to a specifically identified Target for a specified period of time and to provide such materials to the Security Service stated in the authorization.

(2) *Commission* means the Iraqi Communications and Media Commission.

(3) *Compliance Plan*means in this regulation the plan, to be submitted by Providers to the Commission, certifying their ability to comply with all applicable provisions of this Regulation; see Article (VIII)(6) and (7).

(4) *Content* of electronic communications in this regulation means the entirety of the electronic communication transmitted, excluding Traffic Data, but including any and all information and data in whatever form that concerns the substance, purport or meaning of that communication.

(5) *Electronic Communication* means any transfer of aural information, signs, signals, writing, images, sounds, data, or intelligence of any nature, or any combination thereof transmitted in whole or in part by a wire, cable, radio, electromagnetic, photo-electronic or photo-optical system of any type. Electronic Communication includes both Telecommunications and Information Service as defined in this regulation, but excludes, for the avoidance of doubt –

(a) any oral communication uttered by person without any intermediation by any of the systems and processes of the kind described above;

(b) electronic funds transfer information stored by a financial institution in a system used for the electronic storage and transfer of funds; or

(c) Electronic Communications system support services installed and used by Telecommunications or Information Services Providers for internal management, control or operation such as signalling and switching of their respective networks.

(6) *Information Service* has the meaning given this term in Order 65.

(7) *Interception Centre* means a physical location established and operated by the Security Services for the reception and further processing of intercepted Content, Subscriber and Traffic Data, with the handover point for delivery of such databy Providers to the Security Services located here.

(8) *Order 65* means the 2004 Order promulgated by the Coalition Provisional Authority bearing this sequence number, as amended.

(9) *Provider* of Telecommunications or Information Services means a person or entity making available to the any member of the public at large, subject to commercial agreements, its Telecommunications or Information Services, but excludes persons or entities undertaking the provision of Telecommunications or Information Services solely to closed user groups and for private purposes.

(10) *Security Services* means for the purposes of this regulation such federal government security agencies as have been authorized by law to engage in interception and retain Subscriber Data or Traffic Data, including but not limited to the National Intelligence Agency and/or the National Security Apparatus.

(11) *Subscriber* means any person having directly contracted with a Telecommunications or Information Services Provider for the use of services, including but not limited to prepaid as well as post-paid accounts, contracts or similar arrangements, but excluding –

(a) indirect Users, where the Subscriber allows the use of its contracted-for access to third parties; or

(b) anonymous Users such as through the use of public payphones and similar situations or terminal equipment.

(12) *Subscriber Data* means such information as is maintained or required to be maintained by a Provider of Telecommunications or Information Services, including under the provisions of the present regulation, which links the identity of a natural or juristic person to Provider accounts, network identities, services and usage as appropriate to a particular service and including for purposes of subscriber contracting and billing.

(13) *Target* may refer, as the context requires, to a User and/or Subscriber to whose communication Content the interception and/or the turnover of Traffic an/or Customer Data relates and which is authorized by an Appropriate Judicial Authorization directing a Telecommunications or Information Services provider to obtain same under the provisions of this regulation.

(14) *Telecommunications*has the meaning defined for this term in Order 65.

(15) *Traffic Data* means dialling or signalling information that identifies theorigin, direction, destination, and termination of each Electronic Communication generated or received by a Subscriber or User by means of any equipment, facility, or service of a Telecommunications or Information Services Provider.

(16) *User*means in this regulation any person other than a Subscriber using or making use of the Telecommunications or Information Services of a Provider.

Article III. General Obligations

Any Provider of Telecommunications or Information Services must:

(1) Take all appropriate steps to maintain the security, integrity and confidentiality of the Electronic Communications maintained, transmitted or provided to, or by its Subscribers and Users in conformity with the provisions of Articles(IV).

(2) Establish and maintain at all times the capability of its equipment, facilities and/or services that provide a User or Subscriber with the ability to originate, terminate or otherwise direct Electronic Communications to promptly isolate and intercept Communications Content and Traffic Data relating to, or associated with particularUsers or Subscribers and held or carried by such Provider to, or from equipment, facilities or services of such User or Subscriber,concurrently with their transmission in conformity with the provisions of Articles (V) and (VIII) and within the functional and technical parameters specified in SchedulesAand Bof this Regulation; and

(3) To, upon presentation of an Appropriate Judicial Authorization by representatives of the Security Services, promptly intercept, divert and deliver to the Security Service Interception Centre the Target communications Content, and/or Subscriber and/or Traffic Data as specified in the authorization presented, in conformity with the provisions of Article (V).

(4) To securely maintain such electronic records of Traffic and Subscriber Dataas specified in Articles(VI) and (VII) and in accordance with the retention timeframes specified therein.

(5) Devise, implement and document to the satisfaction of the Commission appropriate plans and procedures for carrying out the foregoing matters in accordance with the specifications set out in Article (VIII).The requirements of the foregoing subsections (1) through (5) of this Article do not apply to equipment, facilities, or services that solely support the transport or switching of communicationsfor private networks or for the sole purpose of

interconnecting telecommunications carriers not originating nor terminating electronic communications.

Article IV. Confidentiality of Electronic Communications

(1) Any Provider of Telecommunication or Information Services, including its officers, employees, agents, or subcontractors, may not, other than as specified in sub-sections (2) through(4) below --

(a) intentionally intercept, or attempt to intercept the Content of any Electronic Communication; or

(b) intentionally disclose beyond the Provider entity, its officers, employees and agents, the Contents of, or Subscriber or Traffic Data relating to, any Electronic Communication other than to the person or entity or agent thereof who is the intended addressee or recipient of such Electronic Communication.

(2) It shall not be prohibited for a switchboard operator, or an officer, employee, or agent of a Provider of Electronic Communications whose facilities are used in the transmission of an Electronic Communication, to intercept, disclose, or use that communication where such activity is –

(a) necessarily and unavoidably incident to the rendition of the specific service;

(b) where a switchboard operator or other officer or employee of a Provider becomes aware of a life-threatening emergency and the disclosure thereof made is limited to law enforcement agencies or personnel only; or

(c) for specific network fault or quality monitoring and related purposes only.

(3) It shall not be prohibited for a Provider of Electronic Communications to record and maintain Subscriber and/or Traffic Data, including any such data relating to the use made by Users or Subscribers of its Telecommunications and/or Information Services, including but not limited to such Subscriber and/or Traffic Data as may be required to be collected and retained for purposes of regulatory reporting, including under this Regulation.

(4) It shall not be prohibited for Providers of Electronic Communications, their officers, employees, and agents, to provide information, facilities, or technical assistance to the Security Services authorized by law to intercept Electronic Communications if such Provider, its officers, employees, or agents has been provided with Appropriate Judicial Authorization addressed to the Provider.

(5) No Provider of Electronic Communications, officer, employee, or agent thereof may disclose the existence of any lawful interception or access to Subscriber or Traffic Data,

whether in real time or referring to retained data, including in the context of any Provider records making reference to such matter, except as may otherwise be required by law.

Article V. Interception Capability Obligations

(1) Any Provider of Electronic Communications must ensure that its services, systems, equipment and other enabling technologies utilized for purposes of providing services permit the effective interception of communications Content and Traffic Data pertaining to a specific Subscriber or User by Security Services acting under Appropriate Judicial Authorization. The technical and organizational capabilities required must:

(a) Permit expeditiously isolating the Target communication to the exclusion of all other communication;

(b) Interception and diversion of the communication Content concurrently with their transmission, including their temporary storage if so required;

(c) Interception and diversion of Traffic Data pertaining to the Target communication in such a manner that this Traffic Data may be matched to the interceptedContent to which it pertains before, during and immediately after the Target transmission;

(d) Where applicable, the Provider is responsible for removing any encryption or compression it applied or enabled to be applied to the Target communication, so as to render the Security Services able to use and evaluate Content and Traffic Data intercepted. The Provider is not responsible for removal of any third party encryption unless it possesses the information necessary for its decryption;

(e) Delivery by the Provider of the intercepted Content and Traffic Data to any Interception Centre designated by the Security Services;

(f) Ensuring that all of the foregoing processes are unobtrusive and as undetectable to the Target as possible, while protecting the privacy and security of all Electronic Communications other than the Target communication.

(2) Providers need to ensure that they have the ability to execute the foregoing requirements on a volume basis of no less than [two] simultaneous real-time interceptions for every 10,000 active Subscribers.

(3) Specific functional and technical parameters concerning the interception parameters required are stated in SchedulesAand B of this regulation and incorporated herein by reference.

(4) The capabilities referred to in this Article and the schedules thereto must be in place and fully functional no later than the date on which the Provider files its Compliance Plan

and certification specified in Article (VIII)(6). Failure to meet these requirements may result in sanctions being imposed by the Commission under Article XIIof this Regulation or other lawful basis.

Article VI. Traffic Data Retention Obligations

(1) Providers of Electronic Communication are required to securely maintain, for a period of no less than [one] year from the date of the creation of such information, in an electronic format certain kinds of Traffic Data specified in Schedule A hereto.

(2) The foregoing information is required to be organized in such a manner as to allow for the expeditious search of such information by parameter, and to isolate and identify information associated with a particular Subscriber or User, and be linked to the Subscriber Datarequired to be obtained and maintained by Article VII.

(3) The foregoing requirements are limited in scope as follows:

(a) There is no obligation on Providers to retain communications Content other than to the extent that such Content is inextricably bound up in Traffic Data and may not be segregated as a function of the Provider's systems.

(b) Providers are not required, to collect or create Traffic Data not reasonably available to them, including where Subscribers and Users may utilize "over the top" services not part of the Provider's system or take steps to obscure their communication activities from being recorded by the Provider's systems.

(4) The capabilities referred to in this Article and the schedules thereto must be in place and fully functional no later than the effective date of this Regulation under Article (XIV). Failure to meet these requirements may result in sanctions imposed by the Commission under Article XIIof this Regulation or other lawful basis.

Article VII. Subscriber Data Collection and Retention Obligations

(1) Any Provider of Electronic Communications must, before entering into a commercial relationship, inclusive of any pre-paid services, with a potential Subscriber for the provision of Telecommunications and/or Information Services --

(a) For a natural person, obtain and verify the identity and contact details of any service applicant;

(b) For a juristic person, obtain and verify the identity and contact details of the representative of such entity, including in addition the appropriate authorization of such person to act for the entity, identity registration number and contact details for such entity;

(2) The Provider must ensure that all of the information noted in sub-section (1) and ScheduleCis --

(a) matched to Provider account and other service-relevant identifying numbers issued or enabled by the Provider and uniquely associated with the Subscriber and/or by which the Provider is able to identify that person; an indicative list of such parameters is provided in Schedule Dhereto;

(b) that such matched records are safely and accessibly maintained in electronic, searchable formats by the Provider;

(c) that such records are linked to the information required to be retained under Article VI.

(d) that any change in such information which is brought to the Provider's attention is timely and accurately updated in its records;

(e) That these records are adequately secured and accessible only to authorized personnel of the Provider and, with Appropriate Judicial Authorization, to the Security Services.

(3) Providers of Electronic Communication must retain the above-described records for the entire period for which a Subscriber relationship exists with the Provider and for five years from the date of the termination of the Subscriber relationship, subject to Commission sanctions for non-compliance as stated in Article XII of this Regulation.

Article VIII. MANDATED CARRIER PROCEDURES AND OPERATIONAL STANDARDS

(1) All Providers of Electronic Communications must designate at least one senior officer or employee of the Provider to be responsible for acting as the point of contact by the Security Services and the Commission in any matter relating to the subject of this Regulation, and providing, to the Commission (and where directly requested, the Security Services) with -

(a) The name and a job description/function of the designated senior officer(s) or employee(s) appointed; and

(b) Any information necessary for Security Services to contact this designated senior officer or employee on a seven days a week, 24 hours a day basis, including such alternate or backup points of contact to ensure that no requested interception or access to Traffic Data is delayed.

(2) All Providers of Electronic Communication shall ensure that any interception of communications Content or access to Traffic and/or Customer Data described in Article (V), as well as access to such data retained under the provisions of Articles(VI) and (VII) on or from its network, premises or equipment can be activated only in accordance with Appropriate Judicial Authorization and with the affirmative intervention of the above-noted designated individual officer or employee of the Provider in accordance with the following requirements:

(a) The completion and written documentation of the following steps:

(i.) Determining that the Provider is the addressee of the Appropriate Judicial Authorization;

(ii.) That the Security Service representative delivering such order is able to identify him- or herself as such where the order is delivered in person, or that the sender of the order appears to be a Security Service;and recording the name of the representative or sender of the order;

(iii.) Retaining a copy of the authorization for the Provider's records, along with a written record of date, time, start and stop of interception, the number of records or numbers or circuits affected(asappropriate) and the confirmation of delivery of the information to the requesting Security Service;

(iv.) Adding to such written record the name and position of the Provider officer or employee assisting in this matter, as well as that persons' signature asserting that the record is complete and accurate.

(b) Properly filing and maintaining the above-created record for inspection by, or as the basis of reporting to the Commission for a period of no less than [five]years from the date of its creation, subject to sanctions for non-compliance under Article XII hereof.

(c) Ensuring the security and confidentiality of such record, which shall not be accessible to any person other than the designated officer and employee of the Provider, the Commission, or other government personnel pursuant to the requirements of law or a judicial order.

(d) To ensure that the non-disclosure provisions of Article (IV)(5) are adhered to in respect of such Provider-maintained records; and

(e) Reporting to the Commission, within a reasonable time upon discovery, any act of unlawful interception or access to Traffic Data or compromise of the Provider's security measures to guard against such event.

(3) All Providers of Electronic Communications are required, to develop, as part of their Compliance Plan, policies and procedures put in place to implement the foregoing provisions of this Article.

(4) All Providers are required to file with the Commission, within 30calendar days of the effective date of this regulationa Compliance Plan document setting out, in addition to the matters specified in the foregoing sub-sections,their physical andtechnical readiness to comply with the applicable provisions of this regulation. This Compliance Plan must be signed by at least two or more officers of the Provider and include an affirmative certification of the truth of the statements set out in this Compliance Plan. Incorrect, incomplete or misleading certification may expose the Provider to Sanctions in accordance with Article (XII) of this Regulation.

(5) Upon receipt of such Compliance Plan,the Commission may accept, require revisions, or reject such documentation after its review of the conformity of the materials submitted with the requirements of this Regulation and inform the Provider in writing of this fact, allowing up to 30 days for resubmission of a revised plan.

(6) Providers are required to update and resubmit theirCompliance Plans to the Commission as appropriate when, as a result of changes to the designated staff, contact information for interception, Provider services, network elements or other matters, an updating thereof is required.Any updated information changed by the provider should be clearly marked to facilitate Commission review.

(7) Failure of a Provider to timely and appropriately abide by the provisions of this Article may be sanctioned in accordance with the provisions of Article (XII) of this Regulation.

Article IX. PETITIONS FOR EXTENSIONS OR MODIFICATIONS

(1) Providersprospectively unable to comply for technical or financial reasons with specific provisions of Articles (IV), (V) and (VIII) on the timescales set out in this regulation may petition the Commission for a limited extension of time or other modification setting out a detailed scope of their request and a justification for their request. The filing of a petition will not have the effect of holding in abeyance any obligations of this Regulation until and unless such petition is affirmatively approved by the Commission.

Article X. COOPERATION WITH SECURITY SERVICES IN DELIVERY OF INFORMATION

(1) It is the obligation of the Security Services to supply Providers with the necessary information as to the location of the Interception Centre(s) to which Providers will route intercepted Content and/or Traffic and Customer Data.

(2) Providers having received the above information are bound by the obligations of Article (IV)(5) *mutis mutandis* in respect of any information relating to such Interception Centre(s) as they may have knowledge of.

(3) Providers, having complied with their obligations set out in the foregoing Articles (III) through (IX) and the schedules thereto will be understood to have met their responsibilities under this regulation in each instance of an interception or demand for access to retained data upon confirmed delivery of the requested data to the Security Services Interception Centres in accordance with the requirements of Schedule Ehereto.

(4) Providers are not responsible for the analysis, use, maintenance or any other matter relating to information once delivered to the Security Services as set out in sub-section (3).

(5) The Commission may, upon request of either the Security Services or Providers act as a conduit for information in regard to the matters set out in this regulation, as well as to provide its good offices to settle any disputes between the Security Services and Providers where permitted at law and with the consent of the Security Services.

Article XI. COST ALLOCATION

(1) Providers shall directly procure the systems and/or services necessary to effectuate compliance with the applicable provisions of this Regulation at their own expense.

(2) A Provider may request reimbursement [by the Security Services]for operating costs, but excluding any initial capital costs, incurred as a direct result of fulfilling the mandates of this Regulation[if these in total exceeded 0.5 per cent of audited gross revenues attributable to its Iraqi services in a single calendar year period],where –

(a) The Provider has offered its Telecommunication and/or Information Services to the public on a commercial basis for an uninterrupted period at least as long as the period its claim relates to; and

(b) Providerhas not submitted an analogous claim under the terms of its licence covering the period for which this claim is made.

(3) The Commission is entitled to review and audit any such claim on behalf of any of the relevant Security Services.

Article XII. PENALTIES

(1) Notwithstanding any other regulation or licence provision, the Commission may sanction non-compliance by a Provider with the provisions of this regulation, including but not limited to the following matters:

(a) For non-compliance with the provisions of Article IV, including specifically –

(i.) For any violations of Article (IV)(1)(a), including any attempt, a fine of IQD [20 Million] per instance of such conduct;

(ii.) For any violations of Article (IV)(1)(b), including any attempt, a fine of IQD [10 Million] per instance of such conduct;

(iii.) For any violations of Article (IV)(5), including any attempt, a fine of IQD [10 Million] per instance of such conduct;

(iv.) For any violations of Article (V), where such non-compliance is intentional or grossly negligent, a fine of IQD [10 Million] per interception event affected;

(v.) For any violations of Article (VI), where such non-compliance is intentional or grossly negligent, a fine of IQD [5 Million] per dataset not being made available;

(vi.) For any violations of Article (VII), where such non-compliance is intentional or grossly negligent, a fine of IQD [5 Million] per Customer dataset not being available;

(vii.) For any violations of Article (VIII), where such non-compliance is intentional or grossly negligent, a fine of IQD [10 Million] per interception affected or dataset not available.

(b) For incorrect statements, including but not limited to capabilities, procedures, contact points or information, a fine of IQD [5 Million] per day until compliance is demonstrably achieved.

(2) The Commission may take into account both extenuating and aggravating circumstances, including particularly instances of repeated violations of this regulation, in which case a doubling of the foregoing penalties may be ordered.

Article XIII. TRANSITIONAL PROVISIONS

For the avoidance of doubt, for Providers having been licensed by the Commission prior to the effective date of this regulation and hence subject to licensing terms including the subject matter of this regulation, the terms of this regulation supersede any correspondingprovision of the licence document in accordance with Schedule F hereto.

Article XIV. ENTRY INTO FORCE

(1) This regulation becomes effective on the 30th calendar day following its above-dated approval by the Board of the Commission, or thirty days following its publication by the Commission on its website, if such publication is not contemporaneous, with respect to Providers holding a Commission-issued service licence.

(2) For Providers licensed by the Commission on or after the effective date of this Regulation, the provision of this Regulation become effective on the day such Provider begins offering services on a commercial scale.

Schedule (A): Minimum Interception and Call-Data Retention Parameters

The following parameters are stated in general terms applicable to Telecommunications and Information Services Providers. To the extent that a given Provider's range of services does not encompass certain service providing the parametric requirements stated, the corresponding retention requirements do not apply.			
No.	**Category**	**Parameter**	**Explanatory Note**
1	Transmission Source	Initiating E.164 number	Carrier to match this number to the identity of the Subscriber per Schedule C.
		Initiating User ID	Carrier to match this Carrier to match this User ID number to the identity of the Subscriber per Schedule C for User IDs created by, or known to Provider
		Originating and (where applicable) transiting network identities from which transmission is forwarded to Provider's network	Including but not limited to NSPCs, ISPCSs, MNC or analogous information capable of identifying the carrier/network from which transmission originated and/or through which it was routed
2	Transmission Destination	E.164 number dialled	To be matched to subscriber identity if a Subscriber
		E.164 numbers (and where appropriate services) to which transmission is forwarded, re-routed or transferred; or E.164 number from which transmission is redirected to the Target	To be matched to subscriber identity if a Subscriber
		E.164 numbers added (even if only temporarily) to the transmission	To be matched to subscriber identity if a Subscriber
		Receiving User ID in conjunction with	To be matched to subscriber identity of a Subscriber for User IDs created by, or known to Provider
		IP address(es) of the destination of the	To be matched to subscriber identity if a Subscriber and IP address is located

The following parameters are stated in general terms applicable to Telecommunications and Information Services Providers. To the extent that a given Provider's range of services does not encompass certain service providing the parametric requirements stated, the corresponding retention requirements do not apply.			
No.	**Category**	**Parameter**	**Explanatory Note**
		transmission	on/assigned by Provider network
		Network identities to which transmission is forwarded where it leaves the Provider's network or service area (if appropriate)	Including but not limited to NSPCs, ISPCSs, MNC or analogous information capable of identifying the carrier to which the transmission is forwarded. For mobile carriers, hand-off cell site
3	Transmission Time/Date	Calendar Date	As recorded by Providers' network
		Time Start (transmission(s) and log-in where appropriate)	
		Time Stop transmission(s) and log-out where appropriate	
		Duration(s)	
		Time Zones applicable to above information	
4	Success status	System messages for attempted transmission(s), if any	
		Delivery reports for messages, if any	
5	Service Type & Protocol(s)	Identifiers of the specific service(s), protocol(s) and PDUs used during the transmission	
		For other than telephony transmissions, data volume transmitted	
6	Location	Location(s) of the initiating Subscriber at start/stop of	Best available information available to the Provider – as appropriate

The following parameters are stated in general terms applicable to Telecommunications and Information Services Providers. To the extent that a given Provider's range of services does not encompass certain service providing the parametric requirements stated, the corresponding retention requirements do not apply.			
No.	**Category**	**Parameter**	**Explanatory Note**
	information	transmission	logical/network and/or physical location(s), including Cell ID/location information (for mobile/nomadic services), or installation address for the Subscriber(s) (for fixed services)
		Location of the receiving Subscriber at start/stop of transmission	

٣ Schedule (B): Additional Parameters applicable to Real-time Interception

The following parameters are applicable to real-time interceptions, authorizing both Content Interception as well as access to Traffic Data in addition to those stated in Schedule (A) The following parameters are stated in general terms applicable to Telecommunications and Information Services Providers. To the extent that a given Provider's range of services does not encompass certain service providing the parametric requirements stated, the corresponding retention requirements do not apply.			
No	**Category/Parameter**		**Notes**
1.	An initial unique identifier for the Provider and its interception point		To be provided to the Interception Centre at the start of the transmission
2.	An initial unique transmission-identifying message		
3.	Complete Content of a transmission		To be provided to the Interception Centre interface as a separate Content Channel
4.	All Traffic Data associated with the Target transmission, including, in addition to the Schedule A parameters:		To be provided to the Interception Data interface as a separate Traffic Data Channel
	4.a.	Access-ready status	
	4.b.	All signals emitted by the Target, including post-connection dialled signals emitted to activate features such as conference calling and call transfer or forward;	
	4.c.	All other in-and out-of band network signalling	
5.	Decompression/decryption where provided or enabled by Provider		
6.	Timing signals sufficiently precise to enable the association of Content and Traffic Data channels		
7.	Where appropriate, terminal display information sent and/or received		

٤ Schedule (C): Subscriber Information Required

Minimum Applicant Information to be obtained and verified by any Provider of Electronic Communication before Subscriber Status is granted	
For natural persons	
1	Full name
2	National identity card Number; passport number and issuing country for non-citizens
3	Full Residential and/or business postal address verified by a tax invoice, driving license, rental contract, bank statement or similar document stating such complete address and which was issued within three month of the date of application; for non-citizens not resident in Iraq, at least one address in Iraq.
4	Make and retain a digital copy of the applicant's national identity document (or passport where appropriate) after having verified the match of this document to the applicant
For Juristic Person	
5	All of the foregoing items in lines 1 through 4 for the person acting as the authorized representative of a juristic person, plus
6	Written evidence, on entity letterhead of the representative having been authorized to act for the entity and signed by an officer of the Juristic Person
7	The name of the juristic person as registered
8	Commercial register entry number/register excerpt
9	The registered business address of the juristic person

Schedule (D): Indicative Subscriber-Identifying Variables

The below-identified subscriber-identifying variables are to be matched to the Subscriber Information specified in Schedule (C) and represent a minimum set of variables expected to be available to Telecommunications and Information Services Providers. Depending on the scope of services offered by a particular Provider the available variables may differ.	
1	Telephone number assigned by Provider
2	International Mobile Subscriber Identity (IMSI), or
3	Mobile Subscriber/Station ISDN Number (MSISDN)
4	International Mobile Station Equipment Identity (IMEI) if known to Provider
5	Provider-assigned identities (user names)
6	User-designated identities (user names) if known to the Provider as an incident of providing service
7	IP address where fixed and designated by Provider
8	MAC address(es) of Subscriber equipment where known to Provider

Schedule (E):Security Services Interception Centre Handover Requirements and Arrangements

Provider-sent interception and Traffic Data should be transmitted so as to be compatible with the standards for Law Enforcement Interfaces at Interception Centre(s) set forth in ETSI documents TS 101 671 and ES 201 671 (all components thereof as appropriate to Provider service scope and as per the latest issued version thereof).

Schedule (F):License Provisions Affected

The following provisions of the licenses issued by CMC to date are superseded by this Regulation:

Entity	Article	Clause(s)	Note
Asiacell	23	B through F inclusively	Art 23, Clauses A, G, and H unaffected
ITPC	23	all (A through E inclusively)	--
MunirSuktianInt.'l Group Co.	25	A through E inclusively.	Art. 25, Clauses F and G unaffected
MTC Atheer	23	B through F inclusively	Art 23, Clauses A, G, and H unaffected
Kalimat	25	all (A through E inclusively)	--
Korek	23	B through F inclusively	Art 23, Clauses A, G, and H unaffected
Fanoos	25	all (A through E inclusively)	--

ANNEX 1: COMPARATIVE TABLE OF LICENSE PROVISIONS AND REGULATION TEXT

Substantive License Provisions on Interception	Relative to Draft Regulation on Interception
A. Licensee shall ensure that its Network, systems, equipment and other enabling technologies which Licensee utilizes for purposes of providing Local Telecommunications Services permit the effective interception of communications by permanent (e.g. post-paid) and temporary (e.g. pre-paid) Users of such Services pursuant to technical standards, policies and procedures set forth by the Licensor, which shall be established and amended from time to time in accordance with internationally recognized standards for lawful interception.	Substantively same or superior obligations in regulation, in relation to both pre-and post-paid accounts; Technical parameters called for in license are included in regulation based on international standards.
B. Licensee shall, upon presentation of a duly authorized law enforcement officer of a judicially-granted Warrant Order or Request for Emergency Interception shall:	The regulation provides detailed rules for interception with judicial warrants
i. Initiate a lawful interception in a timely fashion, including prospectively within hours or minutes of receiving a request pursuant to a Warrant Order or Request for Emergency Interception;	The regulation provides more detailed real time interception rules.
ii. Permit the real-time or near-real-time interception of communications;	Covered be the regulation text
iii. Ensure that the communications are intercepted in a reliable manner which fully, accurately and clearly captures the content of the communication, including removing any encryption used for the communication if the Licensee provided or otherwise enabled the use of encryption for the communication;	The regulation provides for both, provision of content and removal of carrier encryption or compression
iv. Securely, effectively and accurately transmit	The regulation provides for carrier

Substantive License Provisions on Interception	Relative to Draft Regulation on Interception
communications that are intercepted pursuant to the technical handover requirements set forth by the Licensor	responsibility for transmission of content and traffic data to handover points in security services interception centres.
v. Provide additional information or data associated with the communication intercepted or the individual or individuals which are the focus of the Warrant Order or Request for Emergency Interception, including:	The regulation makes detailed provisions on the kinds of traffic data to be provided for real time interceptions and in the retained data context.
• *service-related* information or data associated with the communication intercepted, including such information as attempts to initiate, actual initiation, failure to initiate, or termination of the communication by user, dialling or signalling information which timestamps and identifies the origin, direction, destination, handoff or termination of each communications;	Covered in detail
• *user-related information,* including such data as the identity of the individual user targeted and those individuals attempting or actually communicating with the targeted individuals by name, alias, account number, service number, telephone number, facsimile number, email address, IP address or such other identifying information;	Covered in detail, including more precise requirements of user-identifying data to be recorded by providers
• *location-based* information, including the current geographic, physical or logical location of the target identity when intercepted electronic communications are taking place, regardless of whether such is actually taking place, including attempts to utilize electronic communications services and the current geographic, physical or logical location of	The regulation covers this same ground (at left ETSI language modified) in detail.

Substantive License Provisions on Interception	Relative to Draft Regulation on Interception
an identity permanently associated with the target;	
• *other transactional information* associated with the communication; and	Unspecific - no comment
• *additional information* pertaining to the targeted individual(s) held by Licensee, including billing and account records, point-of-sale, sales or marketing information, payment and financial records or other such information.	A data retention requirement including both traffic data as well as transactional customer data such as billing information is included in the regulation
vi. Terminate an interception conducted pursuant to the terms of the Warrant Order or Request for Emergency Interception.	No specific corresponding text in the regulation, but framed in terms of interception to strictly follow the terms of the judicial interception authority, hence same result.
C. The Licensee shall adopt internal policies and procedures relating to the lawful interception of electronic communications which are consistent with, and give full force and effect, to the lawful interception policies and procedures set forth by Licensor and include provisions pertaining to:	The regulation sets out detailed requirements for carrier policies and procedures for the interception context, including the requirement to submit same for CMC review.
i. The identification and appointment of authorized personnel of the Telecommunications Service Provider authorized to facilitate the execution of lawful interceptions of electronic communications and how shall be available upon the request of law enforcement on a 24-hour basis;	Same provision included in regulation.
ii. Procedures for the maintenance of the confidentiality and security of interception methodologies, and the information pertaining to electronic communications intercepted as described herein, including procedures for notifying law enforcement in the event that the	Analogous provisions included in regulation

Substantive License Provisions on Interception	Relative to Draft Regulation on Interception
confidentiality of intercept methodologies the security of information obtained, or the identity of authorized personnel necessary to effectuate lawful interceptions has been compromised.	
D. Licensee shall directly procure the systems and services necessary to effectuate its compliance with the lawful interception requirements set forth above, and those policies and procedures issued from time to time by the Licensor.	Analogous provisions set out in the regulation, though the capability requirements are in this case stated in the regulation.
E. Licensee shall fulfil lawful interception requests received from law enforcement officials pursuant to a duly authorized Warrant Order or Request for Interception at Licensee's own cost. Beginning 360 days following the Effective Date, Licensee may request reimbursement for costs incurred in fulfilling lawful interception requests if such costs exceed 0.5 per cent of its audited gross revenues for the previous calendar year, as calculated in accordance with the requirements [set out elsewhere], payable upon Licensor's independent verification of the Licensee's actual cost to comply with its lawful interception obligations.	Analogous provisions, though (a) effective date shortened, since present carriers are already obligated to comply with similar standards (hence no lengthy transition period needs to be given; and (b) financial contribution mechanism kept, though limited to refer to operational, not capital equipment costs. Please see Section 4, Table 1 concerning the proposed Article XI of the Regulation.
This provision is contained in the license but stated outside the interception terms article in the context of general record-keeping requirements in the license text: All network and performance related data (including QoS performance statistics, call data records, home location registry data and other such information) shall be retained by Licensee for a minimum one (1) year period and all financial records shall be retained by Licensee for a minimum of five (5) years.	The regulation transposes some of the carrier recordkeeping requirements into the interception regulation to ensure their coherence with information retention mandates. The regulation includes more limited provisions since the text at left refers to general recordkeeping, including in other regulatory contexts. In other words, this license text to isto be partiallysuperseded by a specific and detailed requirement to retain traffic data for the same period [one year]

Substantive License Provisions on Interception	Relative to Draft Regulation on Interception
	and customer data for a more extended period (at least fiveyears, including after the end of contract/service period).The license requirement to retain financial data is not to be affected by this regulation.