OfReg DNSSEC Questionnaire Response

QUESTION 1: Provide your views on whether the DNS is 'critical national infrastructure' as defined under the URC Law or 'critical ICT infrastructure' as defined under the ICT Law. Is the location of the physical equipment used to provide DNS services a necessary factor in determining whether the DNS is either 'critical national infrastructure' or 'critical ICT infrastructure'?

Answer 1: Both the URC and ICT laws are sufficiently vague enough to allow DNS to fit under either of them. The location of the physical equipment used to provide DNS services is not a critical factor in determining if it is 'critical national' or 'critical ICT' infrastructure because both laws state that the systems and assets can be physical or virtual and this definition includes cloud services which can be housed globally.

QUESTION 2: Provide your views on whether there are measures other than DNSSEC which can be implemented by ISPs to ensure the integrity of the DNS. If so, explain these measures in detail and provide any relevant documentation.

Answer 2: There are mechanisms available to secure other aspects of DNS but DNSSEC is the globally accepted standard for securing DNS integrity. Langston (2017), Cisco (2018), Chandramouli & Rose (2013)

QUESTION 3: Provide your views on whether the Office should require all ISPs in the Cayman Islands to implement DNSSEC validation services in their networks. What would be a reasonable timeframe to do so? Explain in detail and provide any relevant documentation.

Answer 3: Six months is sufficient time for all local ISPs to commence implementing DNSSEC validation services in their networks. This provides enough time to pull in resources to do the work. Once the ISPs demonstrate their commitment to the process, the initial deadline can be extended without penalty.

QUESTION 4: Provide your views on whether the requirement to implement DNSSEC validation services, if determined by the Office, should be included as a condition in the ICT licences of all ISPs, or included in regulations made by the Office pursuant to section 97 of the ICT Law.

Answer 4: The requirement to implement DNSSEC validation services should be included as a condition in the ICT licences of all ISPs. Leaving the requirement to a regulation should only be considered if accompanied by the will and means to enforce said regulation.

QUESTION 5: Provide your views on the text of the proposed DNSSEC Validation Regulations and, if applicable, a detailed explanation of any proposed changes or differences.

Answer 5: CSD has no issues with the proposed DNSSEC validation regulations.

QUESTION 6: Provide your views on any other matters you consider relevant to this Consultation.

Answer 6: OfReg should consider globally co-locating the .KY DNS servers to reduce existing and additional latency issues introduced by DNSSEC.

CSD would like to see OfReg revisit the idea of letting Uniregistry or any other private entity control the .KY domain.

Introducing any new laws or regulations that cannot be enforced only serves to undermine existing laws and regulations.

References:

Langston, M. (2017) *Six Best Practices for Securing a Robust Domain Name System (DNS) Infrastructure*. Available at: https://insights.sei.cmu.edu/sei_blog/2017/02/six-best-practices-for-securing-a-robust-domain-name-system-dns-infrastructure.html (Accessed: 21 May 2018)

Cisco (2018) DNS Best Practices, Network Protections, and Attack Identification. Available at: https://www.cisco.com/c/en/us/about/security-center/dns-best-practices.html (Accessed: 21 May 2018)

Chandramouli, R. & Rose, S. (2013) https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-81-2.pdf (Accessed: 21 May 2018)

Digicel

DIGICEL CAYMAN ISLANDS

RESPONSE TO:
ICT 2018 – 2 – Consultation DNSSEC Validation

30 May 2018

Digicel thanks the Utility Regulation and Competition Office ("**OfReg**") for the opportunity to submit its comments on the Consultation referred to at caption.

The comments as provided herein are not exhaustive and Digicel's decision not to respond to any particular issue(s) raised in the Comments of other participants in the Consultation or any particular issue(s) raised by any party relating to the subject matter generally does not necessarily represent agreement, in whole or in part nor does any position taken by Digicel in this document represent a waiver or concession of any sort of Digicel's rights in any way. Digicel expressly reserves all its rights in this matter generally.

Digicel

1. Introduction

Digicel refers to the Utility Regulation and Competition Office's ("**OfReg**") document entitled, *Consultation DNSSEC Validation* ("**Consultation Document**"). Digicel welcomes the opportunity to provide its further comments relating to this consultation.

Digicel re-iterates its prior submissions relating to the need for DNSSEC Validation in the Cayman Islands ("**Cayman**"). In particular, Digicel remains of the general view that the OfReg should not mandate the implementation of DNSSEC Validation as a mandatory regulatory requirement in Cayman and hopes further discussions will be held, including face to face meetings, before any final decisions are made by the Of'Reg. Mandatory requirements of this nature will only further harm the industry, and would result in higher costs being incurred by the industry, which costs are likely to be passed down to customers, and may result in barriers to future technological advancements. The information and communications technology industry continues to evolve, with it technological advancements continue to be made, and while imposing a set of systems and requirements may seem to be the correct approach at this time to the Of'Reg, Digicel is of the view that such advancements would mean such systems are likely to become less relevant and in most cases would become redundant. The end result therefore does not justify the time, effort and costs required at this time.

There needs to be further risk analysis conducted, with research specifically conducted within Cayman, before the OfReg seeks to mandate the requirements, as it contemplates in the Consultation Document. Without such reasoned basis, it is difficult to comprehend how the threat to ISPs in Cayman, or such other smaller territories in the Caribbean, would be considered a large scale threat to, as the OfReg claims, critical national infrastructure. There is also a need to properly define and discuss what constitutes "critical national infrastructure" in Cayman, as the present definition and its scope are being disputed as between the OfReg and Licensees. A much more thorough review would also need to be concluded to show that any threats would be so "vital to (the) islands" that its "incapacity or destruction" would in fact have a "debilitating impact on security". Digicel submits that not everything within a national infrastructure sector should be judged as being 'critical'. This therefore raises the need for further market based research and separate set of consultations to discuss what as a matter of fact could be classified as 'critical' within the national infrastructure sector, and the OfReg should look to firstly set out by categorising the sectors into the critical infrastructures, and then identifying how critical something really is to Cayman, and what level of threat it would pose on security, national economic security and public safety.

Digicel also notes with some concern that the OfReg, at paragraph 45 of the Consultation Document, has unilaterally decided that it "considers… the DNS relied upon by ISPs…is critical national infrastructure and critical ICT infrastructure, **whether or not** the…**systems are physically located in Cayman Islands**" [emphasis added]. It is difficult to comprehend how the OfReg has arrived at this conclusion based on its own interpretation of the definition of "critical national infrastructure" and "critical ICT infrastructure", without either further deliberation or consultation with the industry or any properly set out reasons for

concluding as such. Digicel is of the view that if the writers of the URC Law and ICT Law had such an intention, this would have been included within the definition, which presently is not the case. This therefore could only mean that it was always the law-makers intention that reference to infrastructure and systems are to those, which are located in Cayman, whether physically or virtually. The definition itself uses terms such as "islands", no doubt denoting to the Cayman Islands, and "national", which by definition means, "of or relating to **a nation**" [Webster Dictionary Online], and not inclusive of any "international" jurisdiction.

Digicel further submits, respectfully, that any requirements to secure the DNS and protect ISPs from threat should not be mandatory, instead, it should be optional to Licensees, with greater focus on encouraging the Licensees to experiment and adopt solutions that are appropriate, particularly with the changing needs and advancements being made within the industry. This should include looking at more cost effective ways of security implementations. Until this has been properly done, any mandatory imposition or requirement would be premature and may not bring any benefits to Cayman and its people.

Digicel welcomes the OfReg's decision to not pursue modifying ISP Licences in Cayman by making compliance with DNSSEC validation a condition to an operating Licence. Any modification to the Licence must follow the process as set out under the Information Communications and Technology Law (2017 Revision) ("**ICT Law**") at section 31(3), which provides:

> *"(3) Where the Office considers that a licence should be modified the Office shall give to the licensee a written notice that-*
>
> *(a) sets out the proposed modification;*
>
> *(b) states the reasons for the proposed amendment; and*
>
> *(c) invites the licensee to show, within thirty days, why the licence should not be so modified."*

The ICT Law, as it relates to an operators ISP Licence, and as set out above, has its own processes, which must be followed in order to ensure transparency and to provide Licensees with an opportunity to research further, and prepare comments in response to any decision to modify its ISP Licence.

That said, and while Digicel acknowledges that the OfReg has turned to an alternative approach, as set out in section 97(3) (a) (ii) of the ICT Law, which provides the OfReg to make regulations, it is Digicel's view that this alternative can only be employed in circumstances relating to *critical ICT infrastructure*, and Digicel remains of the view that DNS is not a critical ICT infrastructure. The OfReg, throughout this consultation, is yet to provide any reasoned basis to show that DNS is a critical infrastructure as defined under the URC and ICT Laws, respectively, and Digicel remains adamant that it is not. In fact, the OfReg has received submissions discussing this very aspect from both Digicel and Flow, and itself sets out and acknowledges in paragraph 35 of the Consultation Document that neither Digicel nor Flow have "agreed

that DNS should be considered to be critical national infrastructure", and more importantly that, "neither agreed that the Office should mandate the implementation of DNSSEC validation".

As stated in the ICT Law, at section 72(1), ICT network providers should, instead of being forced into implementing the DNSSEC validation, be encouraged to "use best endeavours to ensure that it's respective ICT services and networks" are provided with "due care and diligence". This therefore should be the starting point of any discussion, and any progress made hereon must take such approach into consideration in order to bring out the best result for Cayman and its people. Even if DNS could be classified as a critical national infrastructure, which Digicel does not believe it is, the OfReg is required under section 9 of the ICT Law, "to promote the proper function of the critical ICT infrastructure" and to "develop and maintain cyber security strategies that enhance support of the security and resilience of national and critical ICT infrastructure" in Cayman Islands, and not to force upon the industry regulations or mandatory regulatory requirements, which the industry as a whole does not agree with. Perhaps as a precursor to any final decisions made by the OfReg, it should consider putting together such strategies in a discussion paper, setting out what it believes should be guidelines to be followed by the industry, rather than setting up mandatory regulations.

Finally, Digicel is concerned that paragraph 72 of the Consultation Document states as a matter of fact that the "OfReg **expects to issue a Determination** on the matter addressed" [emphasis added]. This seems to suggest that the OfReg has already predetermined its conclusion to these consultations and that the request for comments from the industry is mere formality. Digicel, however, hopes that this is not the intention of the OfReg, and we welcome further consultation to discuss market research (as well as looking to how this has been dealt with by neighbouring Caribbean islands) conducted in this matter.

Digicel remains grateful to the OfReg for its continued consultative approach relating to matters that would affect the ICT sector and telecommunications industry in Cayman, and welcomes the further opportunity to meet and discuss the matter further, and in greater detail.

To that end, please see below Digicel's comments on the specific consultation questions as set out in the Consultation Document.

2. Consultation Questions

QUESTION 1: Provide your views on whether the DNS is 'critical national infrastructure' as defined under the URC Law or 'critical ICT infrastructure' as defined under the ICT Law. Is the location of the physical equipment used to provide DNS services a necessary factor in determining whether the DNS is either 'critical national infrastructure' or 'critical ICT infrastructure'?

Digicel's views on whether the DNS is 'critical national infrastructure' as defined under the URC Law or 'critical ICT infrastructure' as defined under the ICT Law, has been discussed in the foregoing paragraphs. We trust the views are in order and we hope the OfReg will take into consideration Digicel's reasoned views.

Digicel does not believe that the location of the physical DNS Server, or physical equipment, which is used to provide the DNS Services, is a necessary factor as long as there are redundancies in place, and minimal request delays. Given this, and the fact that DNS Servers or equipment used to provide the Services does not have to be located nationally in Cayman, DNS cannot therefore be a 'critical **national** infrastructure' or 'critical ICT infrastructure', as defined under the respective legislations in Cayman.

QUESTION 2: Provide your views on whether there are measures other than DNSSEC, which can be implemented by ISPs to ensure the integrity of the DNS. If so, explain these measures in detail and provide any relevant documentation.

Digicel is of the view that even with the implementation of DNSSEC validation, the integrity of the DNS may still be under threat. For this reason, focusing only on DNSSEC validation as the only means of protection, and imposing it on the industry as a mandatory regulatory requirement without further and proper research, would not deter cyber-attacks on networks. In fact DNSSEC validation may not protect the integrity of DNS at all. Further investigations and research into other methods should be done, and the only way to do this is to allow the Licensees to implement such necessary safe guards as it sees necessary and to encourage Licensees to develop other ways of ensuring protection. To impose one such measure would not only be costly, but with technological advancement and newer ways found by attackers online, what may be relevant today, may not work tomorrow and would be rendered obsolete. This would come at a cost to Licensees who may refuse future calls to implement measures without proper research and investigation.

For example, even with the DNSSEC validation, there may be a need to implement other protections for DNS, which may include DNS DDoS attacks, or Detect Malware targeting DNS Server. These are however only examples, and Digicel continues to review its own safeguards and remains committed to do its best to implement such measures so as to protect its network, its customers, and to ensure continued resilience.

QUESTION 3: Provide your views on whether the Office should require all ISPs in the Cayman Islands to implement DNSSEC validation services in their networks. What would be a reasonable timeframe to do so? Explain in detail and provide any relevant documentation.

The short answer to the first of these questions is simply 'no'. The OfReg should not require ISPs to implement DNSSEC validation services as a mandatory requirement in their networks. Like many countries worldwide, DNSSEC should be an optional measure and cannot be forced upon Licensees as a mandatory regulatory requirement. We cannot avoid the fact that there are many other security threats to network operators prevalent today especially with evolving technology and new and unfortunately innovative ways cyber-attackers are attacking networks. For this reason operators should be left to determine its own priority measures, and where necessary place higher priority on measures other than DNSSEC. If mandated, it would add further stress to costs and resources, which costs and resources can be put to better use developing other better mechanisms, as well investment in the industry in Cayman.

The question that follows, therefore is redundant as there would be no reason to discuss timeframes, where implementation is not made mandatory. That said, however, theoretically, it may take anywhere between twelve (12) to eighteen (18) months' to reasonably implement DNSSEC. ISPs would need to factor in resource, upgrade and installs to the DNS Server. Given these kinds of timeframes, and the changing network environment and technology advancements, there is not much advantage spending all that time implementing something that may become redundant especially in circumstances where DNS systems are upgraded and also consideration should be given to cyber-attackers who are able to find ways by that time to attack networks regardless of the DNSSEC in place.

QUESTION 4: Provide your views on whether the requirement to implement DNSSEC validation services, if determined by the Office, should be included as a condition in the ICT licences of all ISPs, or included in regulations made by the Office pursuant to section 97 of the ICT Law.

Digicel's views on whether the requirement to implement DNSSEC validation services should be included as a condition in the ICT Licences of all ISPs or included in regulations under the ICT Law have been addressed in the foregoing paragraphs under the heading entitled *Introduction*, and Digicel refers to and relies on those submissions in response to this question.

Further, even if such implementation is required, it must also apply to providers of DNS services for businesses or individuals in Cayman, whether they are locally based or offshore based. It would not be fair to impose any requirements on local ISPs Licences who have largely invested in the future of ICT in Cayman.

QUESTION 5: Provide your views on the text of the proposed DNSSEC Validation Regulations and, if applicable, a detailed explanation of any proposed changes or differences.

By way of Appendix 1 entitled *Draft Administrative Determinations*, the OfReg has pre-determined its conclusion that DNS falls under the definition of being a 'critical national infrastructure' for the purposes of the URC Law and 'critical ICT infrastructure' for the purposes of the ICT Law, and further, qualifies that this applies whether or not such DNS is physically located nationally. Further, by way of Appendix 2 entitled *Draft DNSSEC Validation Regulations Draft Determination,* the OfReg sets out to implement mandatory regulatory regulations relating to the imposition of DNSSEC validation services in Cayman.

Digicel therefore strongly relies on and further iterates its submissions in the foregoing paragraphs in response to such pre-determination and especially in relation to whether DNS can be accepted as a national infrastructure or not, and to submissions relating to Digicel's view relating to the location of DNS, and further to the matter of mandatory regulations relating to this matter.

Digicel's views, as respectfully submitted in the *Introduction* section remains, and Digicel therefore does not accept or see the need for either Appendix 1 or Appendix 2 in its current form, and welcomes OfReg to consult further in this matter and to call face to face meetings to discuss the industries concerns.

QUESTION 6: Provide your views on any other matters you consider relevant to this Consultation.

Digicel relies on submissions made in the *Introduction* section, which sets out its views and opposition to the mandatory imposition of any regulations or modification to Licences in Cayman.

Respectfully Submitted.

Submitted by email to consultations@ofreg.ky

May 31st, 2018

Utility Regulation and Competition Office
3rd floor, Alissta Towers
85 North Sound Rd.
Grand Cayman
Cayman Islands

TO: The Utility Regulation and Competition Office ("OfReg")

RE: ICT 2018 - 2 - Consultation Paper on DNSSEC Validation

As per the consultation request, we are writing to provide the views of WestTel Limited, doing business as, and hereafter referred to as, "Logic" in the Cayman Islands.

QUESTION 1: Provide your views on whether the DNS is '*critical national infrastructure*' as defined under the URC Law or '*critical ICT infrastructure*' as defined under the ICT Law. Is the location of the physical equipment used to provide DNS services a necessary factor in determining whether the DNS is either '*critical national infrastructure*' or '*critical ICT infrastructure*'?

At Logic we believe that the DNS could be considered critical ICT infrastructure and the location of the physical equipment used is not a necessary determining factor.

QUESTION 2: Provide your views on whether there are measures other than DNSSEC which can be implemented by ISPs to ensure the integrity of the DNS. If so, explain these measures in detail and provide any relevant documentation.

DNS Cookies are another potential measure:

https://tools.ietf.org/html/rfc7873

QUESTION 3: Provide your views on whether the Office should require all ISPs in the Cayman Islands to implement DNSSEC validation services in their networks. What would be a reasonable timeframe to do so? Explain in detail and provide any relevant documentation.

At Logic we believe that DNSSEC validation services could be helpful and we think this could be done in the next 12 months.

QUESTION 4: Provide your views on whether the requirement to implement DNSSEC validation services, if determined by the Office, should be included as a condition in the ICT licences of all ISPs, or included in regulations made by the Office pursuant to section 97 of the ICT Law.

We believe that DNSSEC validation services could be helpful.

QUESTION 5: Provide your views on the text of the proposed DNSSEC Validation Regulations and, if applicable, a detailed explanation of any proposed changes or differences.

We recommend a max key length of 5 years.

QUESTION 6: Provide your views on any other matters you consider relevant to this Consultation.

We require a mechanism to upload our keys to ".ky".

Sincerely,

Robert McNabb

CEO