ICT 2018 – 2 - Consultation
DNSSEC Validation

Launch Date: 30 April 2018

Closing Date for Comments: 31 May 2018

Closing Date for Reply Comments: 29 June 2018

Contents

A. Introduction

1. The Utility Regulation and Competition Office (the '***Office***' or '***OfReg***') is the independent regulator established by **section 4(1)** of the Utility Regulation and Competition Law (the '***URC Law***') for the electricity, information and communications technology ('***ICT***'), water, wastewater and fuels sectors in the Cayman Islands. The Office also regulates the use of electromagnetic spectrum and manages the .ky Internet domain.

2. Information and communications technologies are critical to the modern economy and to civil society. All sectors of the economy, including knowledge-based, financial services and tourism, rely upon safe and reliable ICT services to connect customers and suppliers. The public depends heavily on ICT services to connect to each other via media such as telephone, social media and e-mail among others. Any failure of ICT networks and services may therefore have serious consequences for government, businesses and consumers. This is of course the case whether those failures are caused by factors internal to the service providers, such as equipment or process failure, or by factors external to them, such as cyber-attacks.

3. Users of ICT networks and services, consumers and businesses alike, typically do not pay much attention to network security and reliability until the ICT networks or services fail or are compromised. Users often do not realise how dependant they are on these ICT networks and services until they are unable to make a call, access the Internet, watch television, pay for goods using their debit or credit cards, etc.

4. ICT networks are becoming more complex and interconnected. This makes it increasingly difficult to monitor and secure them, which exposes them to greater risk of being compromised or of failing outright. In addition, while legacy network and service platforms may have had features built-in which support network security and reliability, ICT networks are transitioning to Internet Protocol ('***IP***') based technologies which means ICT services are increasingly provided to end-users over the Internet or IP-based platforms. However, IP and the Internet were not necessarily designed with security in mind. Due to increased cyber-attacks on Internet Service Provider ('***ISP***') networks and consumers over those networks OfReg deems it appropriate to consider new approaches for improving network security and reliability.

5. The Office considers that network security consists of policies and practices designed to manage risks to the confidentiality, availability, authenticity and integrity of the network. The Office notes in this regard that the European Union's NIS Directive defines '*security of network and information systems*' as:

> *the ability of network and information systems to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via, those network and information systems*[1]

6. These four elements of confidentiality, availability, authenticity and integrity have different functions in ensuring the security of a network, which can be described at a high level in the following manner: the function of confidentiality is to ensure that a particular message or specific data is available only to the intended recipient of that message or data, and is not accessed by other parties; the function of availability is to ensure that the data, network or other resources can be accessed by users when required; the function of authenticity is to ensure that a message or data in fact originated or was created by the person purporting to originate or create it; and the function of integrity is to ensure that the message or data is accurate and reliable and has not been altered prior to reception by the intended recipient.

7. An ISP may need different measures in order to address each of these aspects of security, and may need different measures for each network layer. A measure designed to ensure the availability of the physical network layer, for example, will not necessarily also ensure the confidentiality of messages generated at the application layers.

8. A critical element of an ISP's network is the Domain Name System ('***DNS***'), as communication over the Internet will not function if the DNS is not operating. The availability of the DNS is, therefore, crucial.

9. However, the authenticity and integrity of the DNS are equally important as they allow users on the Internet to be confident that they are communicating

[1] Directive (EU) 2016/1148 of the European Parliament and of the Council concerning measures for a high common level of security of network and information systems across the Union ('***NIS Directive***'), OJ L 194/1, 06.7.2016, page 13.
http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN

with the domain with which they intended to communicate. Consequently, the authenticity and integrity of the DNS increase public confidence in the use of the Internet to access online services. The Internet Engineering Task Force ('***IETF***') developed a set of protocols, DNS Security Extensions ('***DNSSEC***'), in order to enhance the authenticity and integrity of the DNS.[2] For these protocols to function as intended, ISPs must implement within their networks a process for validating these extensions.

10. The purpose of this Consultation is to set out the Office's proposed determinations in draft as to the implementation of DNSSEC validation services in the Cayman Islands, and to allow persons with sufficient interest a reasonable opportunity to comment on those draft determinations.

B. Background

11. On **5 June 2017**, the Office published the **Notice of ICT 2017 – 1 – Consultation**.[3] The consultation document was intended to solicit information and views from ISPs in the Cayman Islands about DNSSEC and was provided only to the entities currently licensed to operate *Type 9 – Internet Service Provider* ICT services: Cable and Wireless (Cayman Islands) Limited ('***Flow***'), Digicel Cayman Limited ('***Digicel***'), Infinity Broadband Limited ('***C3***'), WestTel Limited ('***Logic***'), United Telecommunications Services Ltd., and the Cayman Islands Government (collectively, '***the Licensees***').

12. On **4 July 2017**, Flow and Digicel submitted their responses to the questions posed by the Office in **ICT 2017 – 1 – Consultation**. On **6 July 2017**, Flow confirmed their response was submitted in confidence and on **15 September 2017** Flow submitted a redacted version of their submission. On **25 September 2017**, Digicel confirmed their submission was not confidential.

13. On **9 October 2017**, the Office forwarded to all ISPs the public versions of the responses from Flow and Digicel and invited Flow and Digicel to submit comments on each other's submissions by **23 October 2017**.

[2] These can be found at http://www.dnssec.net/rfc.

[3] http://www.ofreg.ky/upimages/commonfiles/15064130902017-06-05-Notice-of-Consultation-DNNSEC.pdf

14. In the same letter to the Licensees, the Office posed further questions to all Licensees on network security and on DNSSEC, and posed follow up questions to Flow and Digicel regarding their previous submissions. The Office required responses to the questions by **30 October 2017**.

15. Flow and Digicel did not submit cross-comments on **23 October 2017**. Flow, Digicel and C3 provided their responses to the questions on **30 October 2017** to the Office.

C. Legal Framework

16. In making this consultation document, the Office is guided by its statutory remit, in particular as set out in the URC Law and the Information and Communications Technology Law (2017 Revision) ('***the ICT Law***'), each where applicable. The Office notes the following provisions in particular.

17. **Section 6** of the URC Law states in part:

> *(2) In performing its functions under this Law or any other Law, the Office may –*
>
> *[…]*
> *(d) make administrative determinations, decisions, orders and regulations;*
> *[…]*
> *(k) collect from authorisation holders such information as the Office considers necessary for any one or more of the following purposes –*
> *(i) identifying the geographic position and nature of critical national infrastructure;*
> *(ii) enabling the security and continuity of services over critical national infrastructure; and*
> *(iii) any other prescribed purpose;*
> *[…]*
> *(r) take such action as it considers necessary to ensure the continuity and reliability of operations of critical national infrastructure*
> *[…]*
> *(v) establish and enforce quality of service standards applicable to covered services […]*

18. **Section 2** of the URC Law defines 'critical national infrastructure' to mean:

> *"systems and assets, whether physical or virtual, so vital to the Islands that the incapacity or destruction of the systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters;"*

19. **Section 7** of the URC Law states in part:

> *(1) Prior to issuing an administrative determination which, in the reasonable opinion of the Office, is of public significance, and subject to specific procedures under sectoral legislation, the Office shall –*
>
> *(a) issue the proposed determination in the form of a draft administrative determination;*
> *(b) allow persons with sufficient interest or who are likely to be affected a reasonable opportunity to comment on the draft administrative determination; and*
> *(c) give due consideration to those comments with a view to determining what administrative determination (if any) should be issued.*
>
> *[…]*
>
> *(4) Where the Office intends to issue an administrative determination, the Office shall –*
>
> *(a) give written notice of that intention, to any person with sufficient interest or likely to be affected by the proposed determination; and*
> *(b) afford that person an opportunity to make written representations to show cause why the Office ought not to make such a determination.*

20. **Section 9** of the ICT Law states in part:

> *(1) Subject to this Law, the Office has power to do all things necessary or convenient to be done for or in connection with the performance of its functions under this Law.*
>
> *(3) Without prejudice to subsections (1) and (2), the principal functions of the Office are-*

[…]
(ha) to promote the proper functioning of the critical ICT infrastructure;
[…]
(hc) to develop and maintain cyber security strategies that enhance and support the security and resilience of national and critical ICT infrastructure towards increased economic prosperity, safe and secure business and innovation; […]

21. **Section 72(1)** of the ICT Law states in part:

(1) ICT service providers and ICT network providers shall use best endeavours to ensure that their ICT services and ICT networks are –

(a) reliable;
(aa) where practicable, directly interconnected with each of the other ICT network providers' networks;
(b) provided with due care and skill; and
(c) rendered in accordance with the standards reasonably expected of a competent provider of those ICT services and ICT networks.

22. **Section 2** of the ICT Law defines '*critical ICT infrastructure*' to mean:

"ICT systems and assets, whether physical or virtual, that are so vital to the Islands that the incapacity or destruction of the systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters;"

23. **Section 97(3)** of the ICT Law states in part:

(3) The Office–

(a) after consultation with the Minister, may make regulations relating to –
[…]
(ii) critical ICT infrastructure;
[…]
(b) may make regulations relating to –

[…]
(iii) quality standards; […]

D. Discussion

D.1 Domain Name System

24. The DNS is a distributed network of servers around the globe that translates the domain names in URLs and email addresses used by end-users into the numerical IP addresses that are used on the Internet to locate domains and websites. This process of translation involves multiple steps. When end-users request a domain, for example www.ofreg.ky, their operating system turns to a server known as a 'recursive name server',[4] often located at the user's ISP's offices, for the IP address. The recursive name server turns to another server known as the 'authoritative name server'[5] of the 'root' of the domain, which identifies the authoritative name server of the top-level domain, in this case '.ky'. The recursive name server turns to that second authoritative name server for the identity of the authoritative name server of the second level domain, in this case 'ofreg.ky', and so on, until it obtains from the final authoritative name server the full IP address, at which point it allows the end-user to connect to the domain. This process takes place very quickly and typically appears instantaneous to the end-user.

25. The original DNS system was developed without security in mind. In the early days of the Internet, all elements of the networks, such as academic and military networks, were known to and trusted by each other. Unfortunately, malicious actors can highjack one or more steps of the recursive DNS process and substitute their own IP address for the legitimate address, thereby redirecting the end-user to a false website. The purpose of this malicious activity could be, for example, to facilitate the harvesting of login and password information.

26. Moreover, if the DNS system ceases to function properly or at all, the Internet becomes inaccessible as domain names can no longer be translated into the IP addresses. Without those IP addresses, the routers and servers that make up the Internet cannot know where to send traffic.

[4] So-called because it makes successive requests for information in order to determine the IP address.

[5] So-called because it is the authoritative source of information for a specific root or domain.

For example, the October 2016 attack on the DNS services provided by Dynamic Network Services, Inc. ('***Dyn***') in the United States had a material impact on users of Internet applications by preventing them from obtaining the IP addresses necessary to access those Internet applications.

D.2 DNSSEC

27. Because of the essential role of DNS in the provision of Internet services and the increase in cyber threats to ISPs, OfReg is investigating the implementation of DNSSEC to ensure the integrity of DNS infrastructure. DNSSEC addresses this security issue by using public key cryptography to digitally 'sign'[6] the information sent by the authoritative name servers. When the recursive name server requests the IP address, it also requests the DNSSEC keys associated with the domain. DNSSEC uses a rigid model of a 'chain of trust' from a 'parent zone' to 'child zone', where higher-level zones (such as '.ky') sign or vouch for the public keys of lower-level zones (such as 'ofreg.ky').[7] These keys allow the recursive name server to verify that the information it receives is identical to the record on the authoritative name server. If the recursive name server determines that the address record has been sent by the authoritative name server and has not been altered in transit, it resolves the domain name and the user can access the site. If the IP address record has been modified or is not from the stated source, the recursive name server does not allow the user to reach the fraudulent address. This process of 'DNS validation' allows the end-user to be confident that he or she received the IP address that he or she requested.

28. DNSSEC does not resolve all threats on the Internet. For example, it does not protect against distributed denial of service ('***DDoS***') attacks, ensure confidentiality of data exchanges, encrypt website data, or prevent IP address spoofing and phishing. There are other layers of protection, such as DDoS mitigation, Secure Sockets Layer ('***SSL***') encryption, site validation and two-factor authentication, which are also critical to making the Internet more secure. However, DNSSEC does address a critical

[6] A detailed description of the process of 'signing' a domain is beyond the scope of this letter. At a high level, 'signing' involves adding a prescribed set of records to the information sent by an authoritative name server which the recursive name server can use to verify that the information is legitimate.

[7] The 'child' zone is any domain that sits under a 'parent' zone. For example, a top level domain is the parent zone for a second level domain within that top level domain, and a second level domain is a parent zone for a third level domain within that second level domain.

component of the Internet, as a failure of the DNS system would prevent any use of the Internet.

29. To be fully effective, DNSSEC needs to be deployed across the entire DNS infrastructure. This is because any break in the chain of trust means the end-result of the DNS process, the IP address, cannot be trusted. One of the functions assigned to OfReg by the ICT Law is to act as administrator of the .ky domain. Accordingly, in order to establish the base for the chain of trust, OfReg has ensured that the .ky root is signed. Other organisations have done the same for the roots they manage, such as Verisign in 2010 and 2011 for the .org, .com, .net and .edu roots. The chain of trust also requires that domains, not just roots, be signed and OfReg encourages operators of all domains to do so.

30. However, the effectiveness of DNSSEC does not depend solely on the signing of roots and domains. ISPs must also implement DNSSEC validation within their networks, as this ensures that the DNS process includes the exchange of the DNSSEC keys which verify the integrity of the DNS information and IP addresses sent to the end-user.

31. OfReg does not currently require compliance with DNSSEC but, in light of increased and pervasive attacks against Internet infrastructure and users, is consulting on this matter to consider whether or not it should impose this as a condition upon its Licensees holding an ISP licence.

32. Many ISPs around the world have yet to enable DNSSEC validation and are failing to apply security updates or to correct vulnerabilities in a timely fashion, thereby creating the opportunities for cyber criminals to exploit these vulnerabilities. OfReg considers implementing DNSSEC validation would make it more challenging for cyber criminals to exploit or hijack DNS systems, including within the .ky domain, and would thereby create a more secure environment for local e-Government, e-commerce and general consumer uses of the Internet. As a consequence, OfReg considers it necessary to examine what steps might be taken to protect these aspects of our ICT network infrastructure, economy and population.[8]

[8] The 'WannaCry' cyber-attack in May 2017 showed that many end-users also appear to be failing to apply security updates or to correct vulnerabilities in a timely fashion. While end-user behaviour is important to the security of the Internet, this consultation focuses on ISPs because of their role as intermediaries between end-users and the Internet.

D.3 ICT 2017-1 – Consultation

33. The Office launched **ICT 2017 – 1 – Consultation** to examine the possibility of requiring the Licensees to provide DNSSEC validation services, as a way of ensuring the integrity of the DNS system. The Office noted specifically that:

> *OfReg does not currently require compliance with DNSSEC but, in light of increased and pervasive attacks against Internet infrastructure and users, is consulting on this matter to consider whether or not it should impose this as a condition upon its licensees holding an ISP licence.*

34. As part of that consultation, the Office asked the following questions:

a. *Where are the recursive DNS name servers located that you use to serve your fixed and/or mobile Internet customers in the Cayman Islands? Provide the city and country or territory of the location, as well as the name of the person, entity or other organisation which operates them, if you do not operate them yourself.*

b. *Have you implemented DNSSEC validation in your network?*

c. *Are there any ISPs affiliated with you which have implemented DNSSEC validation in their networks?*

d. *Have you or affiliated companies signed any of the domains which you or those affiliated companies use to provide information to consumers in the Cayman Islands or to contract with customers for the provision of ICT services in the Cayman Islands?*

e. *Describe in detail any other security standards and practices which you have implemented to ensure the security of your DNS infrastructure, the continuity of your services and the management of risk. Please provide supporting documentation.*

f. *Provide your views on whether or not the DNS system, or a specific part of the DNS system, is either 'critical ICT infrastructure' as defined by the ICT Law or 'critical national infrastructure' as defined by the URC Law. Please explain your reasoning in detail.*

g. *Provide your views on OfReg imposing a condition of licence on all Type 9 – Internet Service Provider ICT service licensees requiring them to ensure DNSSEC validation is enabled within the DNS infrastructure (whether or not operated by them) which they use to*

provide Internet services, and to offer that feature, to their customers in the Cayman Islands.

h. *If you have not implemented DNSSEC validation in your network, identify in detail the actions required for you to offer DNSSEC validation to your customers in the Cayman Islands, as well as the time frames and estimated costs of doing so, along with supporting documentation.*

i. *Provide any other views you may have which are relevant to the question of ensuring the security of DNS infrastructure or for protecting your Internet infrastructure, along with supporting documentation.*

35. While the details differed, Digicel and Flow responded to the initial consultation with similar positions when considered at a high level. They noted that they had not implemented DNSSEC validation but described the other security measures they had implemented in their networks. Neither agreed that DNS should be considered to be critical national infrastructure, and neither agreed that the Office should mandate the implementation of DNSSEC validation.

36. The Office addressed three follow-up questions to the Licensees and invited Flow and Digicel to comment on each other's initial submissions. Neither chose to do so, while C3, Digicel and Flow answered the follow-up questions in confidence:

1. *Please describe all measures taken by the Licensee, separately for each OSI layer, to ensure the confidentiality, integrity, authenticity and/or availability of the Licensee's DNS infrastructure. Please explain in detail, separately for each measure, how it addresses confidentiality, integrity or availability of the DNS infrastructure.*

2. *Please describe in detail the specific steps the Licensee would take to ensure continuity of service, in the event its own DNS infrastructure were to become unavailable or were to be compromised. The Licensee's answer should include the process through which its traffic would be redirected to other DNS servers and should identify the other DNS servers it would use.*

3. *Please describe the Licensee's state of readiness for upcoming the Root Zone Domain Name System Security Extensions (DNSSEC) Key Signing Key (KSK) rollover (https://www.iana.org/dnssec/icann-dps.txt), and any measures taken by the Licensee to date to mitigate*

any impact that the KSK rollover might have on the operations of the Licensee.

37. The Office also addressed two additional questions to each of Digicel and Flow, based on their initial submissions. One question, noting the difference between *integrity* and *availability*, asked each Licensee whether it considered "*the measures described in its 4 July 2017 response to be a substitute for DNSSEC validation*." The other question requested information specific to the Licensee. Both Licensees answered these additional questions in confidence.

38. The Office notes that the responses it received from the Licensees were very helpful in understanding the measures they have taken to ensure the security of their networks, including in particular the security of the DNS used to serve users in the Cayman Islands. The Office encourages ISPs to continue their efforts to ensure the security of their networks.

39. The Office notes, however, that no Licensee advised that it had implemented DNSSEC validation services in its network in the Cayman Islands. Further, the Office considers that no Licensee has implemented security measures equivalent to DNSSEC. More specifically, the security measures which have been implemented to-date do not address the authenticity or integrity of the DNS.

D.4 Critical ICT Infrastructure

40. As noted in paragraph 26 above, the Internet becomes inaccessible to users if the DNS system ceases to function properly or at all. The unavailability of the DNS system, i.e. its failure or the failure of links to the system, would prevent access to domains and result in failure of communication across the Internet. The Office notes that some of the Licensees have taken steps to ensure availability, for example, through redundant servers in physically diverse locations.

41. However, events which compromise the integrity of the DNS system can have damaging effects on access to services on the Internet. For example, if the DNS directs traffic intended for one domain to another, communication with the intended domain will have failed and users and their data are at increased risk of being exposed to malicious actors.

42. Lack of access, or unreliable access, to the Internet would have a disastrous effect on the economy of the Cayman Islands, given the country's reliance on effective, secure and reliable communications with the rest of the world.

43. "*Critical national infrastructure*" and "*critical ICT infrastructure*" are both defined in the URC Law and ICT Law, respectively, as "*systems and assets, whether physical or virtual, that are so vital to the Islands that the incapacity or destruction of the systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters*." The Office considers that the unavailability of the DNS, i.e. its "*incapacity or destruction*", would "*have a debilitating impact on … national economic security.*" The Office considers that the loss of integrity of the DNS would have an equivalent effect on national economic security.

44. Because the DNS is so critical to the functioning of the Internet whether in the Cayman Islands or worldwide, OfReg considers, subject to consultation, that DNS is "*critical ICT infrastructure*" under the ICT Law or "*critical national infrastructure*" under the URC Law.

45. The Office notes that the definitions of "*critical national infrastructure*" and of "*critical ICT infrastructure*" simply refer to "*systems or assets, whether physical or virtual*". They do not refer to the location of the systems or assets in question. The Office considers therefore that the DNS relied upon by ISPs in the Cayman Islands is critical national infrastructure and critical ICT infrastructure, whether or not the recursive name servers or associated systems are physically located in the Cayman Islands.

46. Accordingly, the Office proposes to determine, subject to consultation, that:

> **The DNS used by ISPs in the Cayman Islands to provide ICT services to users in the Cayman Islands is '*critical national infrastructure*' for the purposes of the URC Law and '*critical ICT infrastructure*' for the purposes of the ICT Law, whether or not such DNS is physically located within the Cayman Islands.**

47. As discussed in paragraph 5 above, measures taken to enhance the availability of a network component do not necessarily address the integrity, confidentiality or authenticity of that network component. The Office notes that the Licensees have taken steps to ensure the availability of the DNS, for example, by establishing multiple instances of recursive name servers in physically diverse locations. Unfortunately, these do not address the

integrity of the DNS and different measures are necessary, which have not been implemented by the Licensees up until now.

48. The Office considers, therefore, subject to consultation, that it should exercise its functions under **sections 9(3)(ha) and 9(3)(hc)** of the ICT Law and section **6(2)(r)** of the URC Law in respect of DNS.

D.5 Conclusion

49. Based on the foregoing, the Office considers that, while the Licensees have taken steps to ensure the security of their DNS, these steps do not adequately address the authenticity and integrity of their DNS. The Office also considers that, subject to consultation, there are no measures other than DNSSEC which ensure the integrity of DNS.

50. The Office further considers that, subject to consultation, DNS is critical national infrastructure and critical ICT infrastructure, as defined in the URC Law and ICT Law, respectively. The Office considers, therefore, subject to consultation, that it should exercise its functions under **sections 9(3)(ha) and 9(3)(hc)** of the ICT Law and section **6(2)(r)** of the URC Law in respect of DNS.

E. Implementation

51. In light of the considerations set out in Section D.5 above, the Office considers that, subject to consultation, ISPs in the Cayman Islands should be required to implement DNSSEC validation in their networks. The Office notes that it has two principal measures at its disposal to give effect to such a mandate: conditions of licence and regulations.

52. **Section 23(6)(b)** of the ICT Law gives the Office the power to set licence conditions. Further, **section 31** of the ICT Law gives the Office the power to modify licences, subject to consultation with the affected licensees in accordance with the procedures set out in that section, where the Office considers that a licence should be modified.

53. Alternatively, **section 97(3)(a)(ii)** of the ICT Law provides that the Office may, after consultation with the Minister, make regulations relating to critical ICT infrastructure.

54. The Office further notes that its predecessor, the Information and Communications Technology Authority, initiated a consultative process with ISPs in the Cayman Islands on **31 August 2016** regarding proposed Information and Communications Technology Authority (Internet Service Provider Standards) Regulations, 2016 ("***the draft ISP Regulations***").[9] This consultative process has not been concluded and OfReg considers that, if it were to decide to make regulations regarding DNSSEC validation, an option might be to include provisions regarding DNSSEC validation in the draft ISP Regulations.

55. The Office considers that any one of these three approaches would enable it to give effect to the proposed requirement to implement DNSSEC validation.

56. The Office considers that, in these circumstances, incorporating the proposed requirement to implement DNSSEC validation in new, separate DNSSEC Validation Regulations would provide Licensees greater clarity and regulatory certainty as to the requirements in this area.

57. Accordingly, subject to consultation, the Office proposes to determine that "**the Office will make, after consultation with the Minister, the DNSSEC Validation Regulations set out as APPENDIX 2 to ICT 2018 – 2 – Consultation, including the following regulation:**

> **'Each licensee shall implement DNSSEC validation services, as defined in the relevant IETF RFCs,[10] including without limitation RFC 4033,[11] RFC 4034,[12] and RFC 4035,[13] in the ICT network it uses to provide the internet service.' "**

[9] The draft ISP Regulations were proposed pursuant to **section 97(3)(d)** of the Information and Communications Technology Authority Law (2016 Revision), which is now section **97(3)(b)(iii)** of the ICT Law.

[10] See http://www.dnssec.net/rfc.

[11] https://tools.ietf.org/html/rfc4033.

[12] https://tools.ietf.org/html/rfc4034.

[13] https://tools.ietf.org/html/rfc4035.

F. Section 7 Statement

58. As noted above, **section 7(1)** of the URC Law states that prior to issuing an administrative determination of public significance, the Office shall "*issue the proposed determination in the form of a draft administrative determination*."

59. The Office notes that **ICT 2017 – 1 – Consultation** was intended to begin an inquiry into the issue of the security of the DNS and into the possibility of mandating the implementation of DNSSEC validation. As it was more in the nature of an inquiry, that consultation document did not include a draft administrative determination. As a result, the Office will not issue a determination based on **ICT 2017 – 1 - Consultation**.

60. However, the Office considers that measures are required in order to ensure the security of the DNS, based on the information it received from the Licensees during the **ICT 2017 – 1 – Consultation** process. The Office, therefore, proposes to issue the following administrative determinations, set out as draft administrative determinations below and in **APPENDICES 1 and 2**, subject to consultation, after the conclusion of this **ICT 2018 – 2 – Consultation**:

    a. The DNS used by ISPs in the Cayman Islands to provide ICT services to users in the Cayman Islands is '*critical national infrastructure*' for the purposes of the URC Law and '*critical ICT infrastructure*' for the purposes of the ICT Law, whether or not such DNS is physically located within the Cayman Islands.

    b. the Office will make, after consultation with the Minister, the DNSSEC Validation Regulations set out as **APPENDIX 2** to **ICT 2018 – 2 – Consultation**, including the following regulation:

        'Each licensee shall implement DNSSEC validation services, as defined in the relevant IETF RFCs, including without limitation RFC 4033, RFC 4034 and RFC 4035 in the ICT network it uses to provide the internet service.'

61. For the avoidance of doubt, the Office considers the foregoing and the draft DNSSEC Validation Regulations set out at **APPENDIX 2** to be *"draft administrative determinations"* for the purposes of **section 7(1)** of the URC Law.

G. Consultation Questions

62. Based on the above, the Office invites all interested parties to submit their comments, with supporting evidence, on any or all of the following 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*'?

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.

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.

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.

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.

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

H. How to Respond to This Consultation

63. All submissions on this consultation should be made in writing, and must be received by the Office by email to consultations@ofreg.ky by **5 p.m. on 31 May 2018** at the latest. When responding, please repeat the entire question above the corresponding response to each question.

64. The Office expects to publish all submissions received, subject to claims for confidential treatment, by **15 June 2018** and respondents may file reply comments to those submissions on or before **5 p.m. on 29 June 2018** by email to consultations@ofreg.ky.

65. The Office reserves the right not to accept comments or reply comments submitted after these deadlines.

66. Submissions may be filed as follows:

By e-mail to: consultations@ofreg.ky

Or by post:
Utility Regulation and Competition Office
P.O. Box 2502
Grand Cayman KY1-1104
CAYMAN ISLANDS

Or by courier:
Utility Regulation and Competition Office
3rd Floor, Alissta Towers
85 North Sound Road
Grand Cayman
CAYMAN ISLANDS

Or by fax to: (345) 945 8284

67. If a respondent chooses to file any information in confidence with OfReg it should, *at the time of making its filing*, file redacted versions for the public record along with the reasons for each confidentiality claim and the other requirements for confidentiality claims as specified in **section 107** of the URC Law and in the Information and Communications Technology Authority

(Confidentiality) Regulations 2003 (the '***Confidentiality Regulations***').[14] OfReg refers respondents particularly to Regulations 4 (1) (b) and (c) of those Confidentiality Regulations which set out what needs to be included in such a request.

68. The Office reserves the right not to accept requests for confidential treatment which do not comply with the requirements for confidentiality claims, including without limitation the requirement to file a redacted version for the public record at the same time.

69. The Office reminds interested parties that, in accordance with the Consultation Procedures Guidelines,[15] if they choose to apply to the Office for an extension of the time to file comments or reply comments, they must do so *no less than four (4) days before* the day of the existing deadline and include a complete and detailed justification for the request.

70. If applicable, applicants must also copy all other respondents to this consultation *at the same time* as they apply to the Office. The other respondents may comment on the application for an extension within two (2) days of submission of the application, copying the applicant and all other respondents *at the same time*.

71. The Office reserves the right not to accept applications for extensions that do not satisfy these requirements. However, at no time will the Office accept an application for an extension submitted after the deadline in question has passed.

72. OfReg expects to issue a Determination on the matters addressed by this **ICT 2018 – 2 – Consultation** by **the end of 4th Quarter, 2018**.

[14] http://www.ofreg.ky/upimages/commonfiles/1506776718ICTAConfidentialityRegs2003.pdf

[15] See http://www.ofreg.ky/upimages/commonfiles/1507893545OF20171DeterminationandConsultationProcedureGuidelines.pdf.

Appendix 1
–
Draft Administrative Determinations

A. The DNS used by ISPs in the Cayman Islands to provide ICT services to users in the Cayman Islands is '*critical national infrastructure*' for the purposes of the URC Law and '*critical ICT infrastructure*' for the purposes of the ICT Law, whether or not such DNS is physically located within the Cayman Islands.

B. The Office will make, after consultation with the Minister, the DNSSEC Validation Regulations set out as **APPENDIX 2** to **ICT 2018 – 2 – Consultation**, including the following regulation:

> 'Each licensee shall implement DNSSEC validation services, as defined in the relevant IETF RFCs, including without limitation RFC 4033, RFC 4034 and RFC 4035, in the ICT network it uses to provide the internet service.'

Appendix 2
–
Draft DNSSEC Validation Regulations
Draft Determination

THE INFORMATION AND COMMUNICATIONS TECHNOLOGY LAW (2017 REVISION)

THE INFORMATION AND COMMUNICATIONS TECHNOLOGY (DNSSEC VALIDATION) REGULATIONS, 2018

The Office, in the exercise of the powers conferred by section 97 (3) (a) (ii) of the Information and Communications Technology Law (2017 Revision), makes the following regulations-

Citation

1. These regulations may be cited as the Information and Communications Technology Law (DNSSEC Validation) Regulations, 2018.

Definitions

2. In these regulations-

"DNS" means Domain Name System;

"DNSSEC" means DNS Security Extensions;

"DNSSEC validation" means the process applied by a licensee's ICT network to confirm the authenticity and integrity of the DNS information received by the licensee's ICT network;

"IETF RFC" means a Request for Comment published by the International Engineering Task Force;

"internet service" means a Type 9 *Internet Service Provider* ICT Service, as defined from time to time in the Notice gazetted pursuant to section 23(2) of the Law.

"Law" means the Information and Communications Technology Law (2017 Revision) or its equivalent;

"licensee" means a Licensee under the Law that holds a Type 9 *Internet Service Provider* ICT service licence as defined from time to time in the Notice gazetted pursuant to section 23(2) of the Law;

DNSSEC Validation

3. Each licensee shall implement DNSSEC validation services, as defined in the relevant IETF RFCs, including without limitation RFC 4033 and RFC 4034, in the ICT network it uses to provide the internet service.

Effective Date

4. The DNSSEC validation services referred to in regulation 3 shall be implemented no later than […] months after these Regulations come into force.

Made in Cabinet the […] day of […], 2018

[ ]
Clerk of the Cabinet