Office of Utilities Regulation

Outage Reporting Protocols and Measures to Improve Network Resiliency in Disasters

Consultation Document

OFFICE OF UTILITIES REGULATION

2022 June 20

Abstract

Under the Telecommunications Act and the Office of Utilities Regulation Act, the Office of Utilities Regulation has, among other tasks, the encouragement of competition and the protection of the interests of consumers. Over the past years, Jamaica has experienced several significant outages affecting both mobile and fixed networks and services. These have increased public awareness and concern about the reliability of telecommunications. As consumers become increasingly reliant on telecommunications for personal and commercial use, the quality of telecommunication services delivered to the public assumes even greater significance.

Promoting the reliability and resiliency of telecommunications networks and services, and ensuring a minimum standard of quality is key to protecting consumers. Accordingly, the OUR intends to establish an Outage Reporting Protocol (hereinafter, the "Protocol" or "Protocols") that will provide the OUR with the data required to assess the magnitude of outages, monitor service restoration activities, and identify common recurrent threats to the normal functioning of networks and services. Such a tool is also aimed at ensuring that an in depth analysis of the root cause(s) of each outage is executed, and that the necessary countermeasures are taken by service providers to mitigate the risk of recurrences.

The resiliency of telecommunications networks is even more critical during an emergency, such as disasters (natural and man-made). While the OUR acknowledges the leading role of the Office of Disaster Preparedness and Emergency Management in disaster management, the OUR believes that adding provisions to the Protocol that specifically address disaster situations may help significantly in the different phases of a disaster.

Consultation Process

Persons who wish to express opinions on this Consultation Document are invited to submit their comments in writing to the Office of Utilities Regulation ("OUR") by post, delivery, facsimile or email addressed to:

Office of Utilities Regulation
P.O Box 593
36 Trafalgar Road
Kingston 10

Attention: Marsha Minott

Fax: (876) 929-3635
Email: QoSProject@our.org.jm and Cc: rim@our.org.jm

Responses are requested by 2022 July 18

Any confidential information should be submitted separately and clearly identified as such. The submission of confidential information should be accompanied by a detailed justification in keeping with section 7(6) of the Telecommunications Act.

Responses that are not confidential, pursuant to sections 7(6) and 7A of the Telecommunications Act, will be posted to the OUR's website (http://www.our.org.jm/). Respondents are therefore requested, where possible, to supply their responses in electronic form to facilitate such postings.

Comments on Responses

The OUR's intention in issuing this Consultation Document is to stimulate public debate. The responses to this Consultation Document re a vital part of that public debate. There will therefore be a specific period for respondents to view other responses (non-confidential) and to make comments on them. The comments on responses may take the form of either correcting a factual error or putting forward counterarguments and/or providing relevant data in support of an argument or counterargument. As in the case of the responses, comments which are not confidential pursuant to the Telecommunications Act will be posted to the OUR's website.

Comments on responses are requested by 2022 August 2

Consultative Timetable

The timetable for this consultation is summarized below:

Event	***Date***
Publish Consultation Document	2022 June 20
Receive Responses to Consultation	By 2022 July 18
Receive Comments on Responses	By 2022 August 2
Issue Determination Notice	By 2022 November 30

Contents

Chapter 1. Introduction

1.1. Background

1.1.1 Consumers purchase telecommunications services from service providers, with a reasonable expectation that they will receive quality service. As consumers become increasingly reliant on telecommunications for personal and commercial use, the quality of telecommunications services becomes fundamental. The Office of Utilities Regulation (hereinafter, the "OUR" or "the Office") has noted an increase in consumer complaints concerning the quality of telecommunication services. The complaints received by the OUR highlight several quality of service issues on the telecommunications networks including frequent outages.

1.1.2 Jamaica has experienced several significant outages on both mobile and fixed networks in recent times, which have increased public concern about the reliability of telecommunications services. The OUR is concerned about the prevalence of these issues and their impact on the overall quality of service received by customers. Reliability is widely recognised as a key variable that contributes to the overall quality of a product. It becomes increasingly important in a market when the cost of downtime and maintenance results in financial burdens for consumers. In Jamaica, for instance, failure of a telecommunications network is costly particularly for the financial and business processing outsourcing sectors.

1.1.3 Telecommunications services play a vital role in emergencies and disasters as they facilitate access to emergency and rescue services as well as support relief operations. Telecommunications services also provide a means for the dissemination of alerts and updates.

1.1.4 Axon Partners Group Consulting S.L.U. (hereinafter, "Axon") has been commissioned by the OUR to provide consulting services in relation to initiatives aimed at improving the quality of service/experience (QoS/QoE) of telecommunications services.

1.1.5 One such initiative is the implementation of outage reporting protocols and disaster resiliency measures for the telecommunication sector. The outage reporting protocols will ensure timely notification and that a requisite analysis is carried out for outages in telecommunications networks and services, while the

disaster/emergency related measures are aimed at ensuring continuity of operations in emergency/disaster situations.

1.1.6 To facilitate this initiative, Axon analysed outage reports submitted to the OUR by Licensees and assessed the process of discovery and/or notification of such events, as well as the subsequent process of analysis of the root causes that contributed to such outages. The key takeaways from this review are summarised below:

- In general, outage reports were submitted by the affected Licensee without adhering to any notification procedure and without any pre-defined schedule.
- The content of such outage reports did not follow a standard format, although a template was eventually adopted by some Licensees.
- The root cause and scope of the outage were difficult to determine in the early stages of the investigation and changed in some cases as the investigation progressed.
- Ensuing discussions between the affected Licensees and the OUR, revealed discrepancies on the reported diagnosis of the outage, and the countermeasures required to mitigate its recurrence.
- The outage investigation process was often lengthy, lasting for months or years, and in some cases, ended with no definitive result regarding the root cause of the outage.

1.1.7 In its review of reports on recent outages, the OUR has observed that they lacked standardised notification procedures, a gap that justifies the OUR's proposal to implement standard outage reporting protocols. The OUR is of the view that defining a standard content for outage reports will also help Licensees in reporting the details of the outage more thoroughly, thereby speeding up the discussion and contributing to the removal of the root cause and preventing future outages.

1.1.8 The definition of a standard outage reporting protocol is framed within the scope of QoS regulations. In line with international recommendations, the OUR is of the view that greater transparency on the performance of telecommunications networks and services contributes to increasing competition in the market, and helps users make informed choices regarding their telecommunications service providers.

1.1.9 The resiliency of telecommunications networks becomes even more critical in the course of responding to an emergency, such as a disaster. In the case of disasters,

the resilience and redundancy of telecommunications networks is critical in all the different phases of disaster management. The Office of Disaster Preparedness and Emergency Management (hereinafter, the ODPEM), which is the entity responsible for disaster management in Jamaica, has been given the mandate of taking action to reduce the impact of disasters and emergencies on the Jamaican population and its economy. However, the OUR is of the view that there are some issues related to emergency/disaster management which can be addressed under its remit. The OUR has therefore proposed for inclusion in the Protocol, provisions which will be relevant in different phases of an emergency/disaster.

1.2. Basis

1.2.1 This consultative document presents a draft Outage Reporting Protocol (hereafter "the draft Protocol") and measures aimed at improving resiliency in times of emergency/disasters. The document also summarises the assessment carried out by the OUR to ensure that the proposed draft Protocol and measures were developed in accordance with international best practices. The draft Protocol and the resiliency measures proposed in this document are influenced by investigations undertaken and consultations held with various stakeholders. Specifically, the proposals are influenced by:

- Discussions with government agencies, consumer organisations, and service providers
- Analyses of outage reports sent to the OUR
- Responses to information requests from the OUR to Licensees
- International benchmarks

1.2.2 In general, the draft Protocol and resiliency measures build on the capabilities of the OUR to:

- Require adherence to standards by Licensees
- Obtain information from service providers by formal information requests
- Examine documents
- Make available to the public, information concerning matters relating to the telecommunications sector

1.2.3 The objective of these proposed measures is to ensure that:

- the Office is properly informed, and in a timely manner, of any relevant disruption in telecommunication services and the steps being taken to restore service;
- a proper assessment of disruptions is undertaken and appropriate corrective actions are taken to prevent a recurrence of a disruption of a similar nature;
- end-users are informed of any planned and/or unplanned outages.
- there is continuity of operations in cases of emergency situations such as disasters.

1.3. Structure of the Consultation Document

1.3.1 The Consultation Document is structured as follows:

- Chapter 2Legal framework outlines the Legal Framework that underscores the remit of the OUR in regard to the establishment of a quality of service framework.
- Chapter 3 provides a summary of the review of internationally accepted practices.
- Chapter 4 provides an explanation of the topics most relevant to the draft Protocol and resiliency measures.
- Chapter 5 provides a Summary of questions.
- Annex A presents the Draft Outage Reporting Protocol.

Chapter 2. Legal framework

2.1.1 The OUR was established pursuant to the Office of Utilities Regulation Act (the OUR Act) with the power to regulate "*prescribed utility services*." Section 2 and the First Schedule of the OUR Act define "*prescribed utility services*" to include "*the provision of telecommunication services.*"

2.1.2 The power and authority of the OUR to regulate the telecommunications sector is governed by the provisions of both the OUR Act and the Telecommunications Act (the Act).

2.1.3 Section 4(3) of the OUR Act in particular empowers the OUR to undertake such measures, as it considers necessary and desirable, to inter alia:

"(a) encourage competition in the provision of prescribed utility services;

(b) protect the interests of consumers in relation to the supply of a prescribed utility service;

…

(d) promote and encourage the development of modern and efficient utility services; …"

2.1.4 The Act also grants specific powers to the OUR to provide regulatory oversight on certain areas of focus including, but not limited to, quality of service standards and consumer protection in the provision of telecommunications services. Extracts of some of the relevant provisions of the Act are set out below:

"4 – (1) The Office shall regulate telecommunications in accordance with this Act and for that purpose the Office shall –

(a) regulate specified services and facilities;
...
(d) promote the interests of customers, while having due regard to the interests of carriers and service providers;
...
(f) make available to the public, information concerning matters relating to the telecommunications industry;

(g) promote competition among carriers and service providers;
...
(3) In exercise of its functions under this Act, the Office may have regard to the following matters –

(a) the needs of the customers of the specified services;

(b) whether the specified services are provided efficiently and in a manner designed to –

…

(iii) afford economical and reliable service to its customers;

(c) whether the specified services are likely to promote or inhibit competition"

2.1.5 Under Section 4(4) of the *Act* the OUR has the authority to require a service provider to supply records, documents or other information in relation to that Licensee's operations, within such reasonable time and for such reason, as the Office may specify

Chapter 3. Investigation of internationally accepted practices

3.1. Introduction

3.1.1 This chapter provides some insights on the review carried out by the OUR to ensure that the proposed draft Protocol and resiliency measures are aligned with international best practices. For that purpose, the following sections provide information on:

- The scope of the review, in terms of its topics and the countries compared (section 3.2).
- A comparison to similar initiatives in other countries (section 3.3).
- A summary of the key takeaways from this analysis (section 3.4).

3.2. Scope

3.2.1 In order to ensure that the proposed outage notification protocol and resiliency measures are in line with the international best practices, the OUR has analysed how other countries deal with the following key topics:

- **Categorisation of outages**. Outages of different categories may require Licensees to meet different reporting deadlines depending on their severity or the criticality of their impact.
- **Responsible person and means of communication.** This looks at entities or individuals that must be notified in the event of an outage, and the manner in which these notifications and outage reports must be conveyed.
- **Reporting procedure .** These include the reports that should be prepared and submitted in the event of an outage; the mandatory and recommended contents to be included in such reports at each stage of the process, and the timeframes for the submission of the report.
- **Sanctions.** These are penalties applicable to Licensees if they fail to meet their obligations regarding outage reporting.
- **Resiliency measures**. These are measures to increase the resiliency of telecommunication networks in disasters.

3.2.2 The information provided by service providers in response to the OUR's 2021 November 02 Request for Information (RFI) were analysed. The aim of this RFI was to collect information regarding the standard operating procedures (SOP) of telecommunications service providers in Jamaica in circumstances where there are service interruptions and/or unplanned network outages.

In particular, service providers were requested to provide information on:

(a) how network outages are usually detected;

(b) whether they categorise outages and how;

(c) any processes put in place for the restoration of services;

(d) whether they notify the OUR and/or end-users;

(e) whether they perform root-cause analyses (RCA); and

(f) whether the company has a disaster management plan.

3.2.3 The related rules and protocols from eight (8) countries worldwide were analysed for the purpose of designing the outage reporting protocol. Exhibit 1 lists the countries considered, as well as the references and links (last accessed 2022 January) to the documents analysed.

Country	ISO3	Flag	Consulted document
Jamaica	**JAM**		Information collected from telecommunications service providers in response to the RFI sent to operators on 2021 November.
Cayman Islands	**CYM**		*ICT Outage Reporting Rules* (Link)
Dominican Republic	**DOM**		*Norma de calidad del servicio de telefonía y acceso a internet* (Link) [Telephony and internet access quality of service standard]
Chile	**CHL**		*Decreto 60 – Reglamento para la interoperación y difusión de la mensajería de alerta, declaración y resguardo de la infraestructura crítica de telecomunicaciones e información sobre fallas significativas en los sistemas de telecomunicaciones* (Link) [Decree 60 - Regulations for the interoperation and dissemination of alert messaging, declaration and safeguarding of critical telecommunications infrastructure and information on significant failures in telecommunications systems.]
United Kingdom	**GBR**		*Ofcom guidance on security requirements* (Link)
Finland	**FIN**		*Regulation 66 on disturbance in telecommunications services* (Link)
Switzerland	**CHE**		*Technical and Administrative Regulations concerning Reporting of Network Faults* (Link)

Country	ISO3	Flag	Consulted document
Qatar	**QAT**		*Quality of retail communication services provided to the public regulation*[1] (Link)
Lebanon	**LBN**		*Technical Quality of Service and Key Performance Indicators Regulation* (Link)

Exhibit 1: References and consulted documents used in the gap analysis for outage reporting protocols [Source: Axon]

3.2.4 Additionally, the following documents and regulations were analysed for the purpose of proposing measures to increase the resiliency of telecom networks in disasters:

Country/Org	ISO3	Flag	Consulted document
Jamaica	**JAM**		Information collected from telecommunications service providers –– in response to the RFI sent to operators on 2021 November 02.
Bahamas	**BHS**		Disaster Management Regulations for the Electronic Communications Sector in The Bahamas (Link)
Trinidad and Tobago	**TTO**		Consultative document on the National Emergency Communications Plan (Link)
Maldives	**MDV**		Maldives Telecommunication Policy 2006-2010 (Link)
United Kingdom	**GBR**		Guidance on Telecoms resilience (Link)
International Telecom. Union	**ITU**		ITU Guidelines for national emergency telecommunication plans (Link) Guide to develop a telecommunications/ ICT contingency plan for a pandemic response (Link)
ENISA	**ENI**		European Union Agency for Network and Information Security (ENISA) Report on *National Roaming for Resilience* (Link)

Exhibit 2: References and consulted documents used in the gap analysis about resiliency of telecom networks in disasters [Source: Axon]

3.3. International comparison

3.3.1 This section provides some insights on the key topics outlined in paragraph 3.2.1 for the countries reviewed and compares the status in Jamaica to international best practice.

[1] This document is subject to public consultation.

Categorisation of outages

3.3.2 Exhibit 3 presents a summary of the categorisation of outages found in international practices and in the Jamaican service providers' reporting procedures.

Country	Summary of the assessment
Jamaica 	It is a common practice among Jamaican service providers to categorise outages. In particular: ▶ One operator stated that it categorises outages based on the number of nodes affected and defines three (3) outage categories. ▶ Four operators stated that they categorise outages according to the severity and scope of the outage. Categories defined range between two (2) to four (4) tiers. ▶ One operator stated that it categorises outages based on their nature and defines three (3) outage categories. ▶ One operator stated that it only distinguishes between planned and unplanned outages.
Cayman Islands 	Three categories are defined in the Rules: ▶ Reportable Outages are those of at least 15 minutes duration that potentially: • Affect at least 50 subscribers • Affecting Special Offices and Facilities, such as airports, seaports, as well as emergency services, key government and private facilities specified by the Office • Mission Critical Outages ▶ Mission-Critical Outages means those critically affecting the national security/emergency preparedness (NS/EP) operations and facilities of the Police, the Armed Forces, Fire Stations, hazard management, and Emergency Medical Centres. ▶ Non-Reportable Outages are those that do not meet the former requirements. ▶
Dominican Republic 	Two categories are defined, namely, ▶ Type 1 (non-reportable): A single user is affected. ▶ Type 2 (reportable): More than 5% of the customer base or 30k users are affected.
Chile 	Three categories are defined, namely, ▶ High impact: Any fault: i) affecting critical infrastructure of level 1, ii) impeding the broadcast of emergency communications, and iii) affecting 30% of the subscribers within one or more regions. ▶ Medium impact: Any outage not deemed to have high impact that affects 100% of the subscribers within one or more communes. ▶ Low impact: Any outage not deemed to have high or medium impact, that affects 20k subscribers or five or more access sites.

Country	Summary of the assessment
United Kingdom 	Three (3) categories are defined, namely, ▶ Urgent: Incidents i) causing major cybersecurity breaches, ii) affecting 10M users or 250k users within 12 hours, iii) attracting mainstream media, and iv) affecting critical infrastructure. Urgent incidents are reportable incidents with higher priority. ▶ Reportable: Incidents not deemed as urgent, but i) reported by other government agencies, ii) causing cyber security breaches, iii) include repeated incidents, iv) affect the ability of the customer to contact emergency services, or v) meet certain numerical thresholds in terms of subscribers affected. ▶ Non-reportable: Incidents not deemed to be urgent or reportable.
Finland 	Four (4) categories are defined, ranked from high-to-low. ▶ A: The disturbance prevents the operation of: i) telephony services of more than 100k users, ii) internet access services of more than 200k users, iii) any of the previous service of more than 25k users within more than 60,000 km^2, iv) SMS service of more than 200k users, v) e-mail service of more than 500k users, vi) 500 base stations. ▶ B: The disturbance prevents the operation of: i) telephony services of more than 10k users, ii) internet access services of more than 50k users, iii) any of the previous service of more than 20,000 km^2, iv) SMS service of more than 50k users, v) e-mail service of more than 200k users vi) another communication service of more than 200k users, vii) 100 base stations. ▶ C: The disturbance prevents the operation of: i) telephony services of more than 1k users, ii) internet access services of more than 1k users, iii) SMS service of more than 1k users, v) e-mail service of more than 50k users, vi) another communication service of more than 50k users, vii) 10 base stations. ▶ D: A disturbance not deemed A, B, or C.
Switzerland 	Two (2) categories are defined, namely, ▶ Reportable faults: Faults: i) lasting for more than one hour, ii) completely interrupting or markedly restricting a service, iii) affecting public telephone services, emergency services, data transmission networks/services and broadcasting, and iv) exceeding certain thresholds for each type of service. ▶ Non-reportable faults: Faults not deemed to be reportable.
Qatar 	Two (2) categories are defined, namely ▶ Notifiable fault: 10% of end-users and/or traffic are affected. ▶ Non-notifiable fault: Faults not deemed to be notifiable.
Lebanon 	Three (3) categories are defined, namely, ▶ Minor: Outages affecting individual sites and/or components at the edge of the network. Service is not interrupted. ▶ Major: Outages affecting a part of the network and influencing less than 30% of the traffic. ▶ Critical: Outages affecting the entire network, any core component, and greater than or equal to 30% of the traffic. Network outage occurring during normal working hours.

Exhibit 3: International benchmark review regarding categories of outages [Source: Axon]

3.3.3 All countries included in the benchmark provide some kind of categorisation of outages, as do telecommunications service providers in Jamaica. However, there

are differences between the categories defined across the countries covered by the review. One-half of the countries in the benchmark only define conditions for outages to be reported, thereby considering only "*reportable*" and "*non-reportable*" outages in practice. The remaining countries however go one step further and define different reportable categories, based on the scope and impact of the outage.

3.3.4 Additionally, differences in these countries' definition of criteria for the categorisation of outages can also be observed. The following exhibit summarises the factors used by each country to determine categories of outages.

Criteria	JAM	CYM	DOM	CHL	GBR	FIN	CHE	QAT	LBN
Impact on critical/special infrastructure	✓	✓	✗	✓	✓	✗	✗	✗	✗
Impact on emergency communications	✗	✗	✗	✓	✓	✗	✓	✗	✓
Level of the network affected (e.g., core or access)	✓	✗	✗	✓	✗	✗	✗	✗	✓
Expected duration of the outage	✗	✗	✗	✗	✓	✗	✓	✗	✗
Services affected	✓	✗	✗	✗	✗	✓	✓	✗	✗
Number of users affected	✓	✓	✓	✓	✓	✓	✓	✓	✗
Percentage of traffic affected	✗	✗	✗	✗	✗	✗	✗	✓	✓
Number of regions affected	✗	✗	✗	✓	✗	✗	✗	✗	✗
Impact on broadcast media	✗	✗	✗	✓	✗	✗	✗	✗	✗
Nº access nodes or sites affected	✓	✗	✗	✓	✗	✓	✗	✗	✗

Exhibit 4: International benchmark review regarding categorisation criteria [Source: Axon]

3.3.5 As shown in Exhibit 4, the number of affected users is the most widely used criterion for rating the severity of network outages. The number of nodes affected and the level of the network, i.e., whether it affects core communication nodes is used in half of the countries. Further, one-half of the countries take into consideration whether the outage affects critical/special infrastructure or emergency communication services when stating that an outage is critical.

Responsible person and means of communication

3.3.6 International references show that service providers typically notify to the relevant authority (National Regulatory Authority (NRA), emergency coordinator, etc.) the occurrence of an outage. Further, in some cases, the protocols include clauses for notifying end users.

Roles and means	JAM	CYM	DOM	CHL	GBR	FIN	CHE	QAT	LBN
Notification to the relevant authority (e.g., NRA, emergency coordinator, etc.)									
Person in charge of the communications	Not defined	Approv. SPOC[2]	Not defined	Emerg. Coord.	Approv. SPOC	Not defined	Not defined	Not defined	Not defined
Does the protocol define any means of notification?	✓	✓	✗	✗	✓	✓	✓	✓	✗
Online submission	✗	✓	N/A	N/A	✗	✓	✗	✗	N/A
E-mail submission	✓	✗	N/A	N/A	✓	✓	✓	✓	N/A
Phone	✓	✗	N/A	N/A	✓	✓	✓	✗	N/A
Other	Not defined	Not defined	N/A	N/A	Not defined	Not defined	Not defined	Web, SMS	N/A
Notification to end-users									
Does the protocol define any means of notification?	✓	✗	✓	✗	✗	✓	✗	✓	✗
Mass communication media (i.e., TV, press, radio)	✓	N/A	✓	N/A	N/A	✗	N/A	✗	N/A
Other media (e.g., SMS, W'App, IVR, e-mail, website)	✓	N/A	✓	N/A	N/A	✓	N/A	✓	N/A

Exhibit 5: International benchmark study regarding roles and means of communication [Source: Axon]

3.3.7 Only four (4) of the benchmark countries clearly define who is in charge of notifying an outage to the relevant authority. The outage reporting protocols of the Dominican Republic, Qatar, and Lebanon are defined within their corresponding QoS frameworks and do not specify details about the person in charge of notifying

[2] Single point of contact.

the relevant authority. Communications regarding outages usually occur via e-mail, although notifications via phone call are often used as a solution of last resort in United Kingdom, Switzerland, and Finland (in the latter, they are often the preferred option for critical outages).

3.3.8 On the other hand, the communication of an outage to the public in general is defined within the regulations of three (3) of the benchmark countries. In these cases, mass communication channels (i.e., TV, press, radio) are the preferred choice to notify end-users.

Reporting procedure

3.3.9 The notification of an outage to the relevant authority is usually done by means of a multi-step process. Exhibit 6 summarises the different reporting stages and the typical timeframes found in international practice for the submission of outage reports.

Reporting stage[3]	JAM	CYM	DOM	CHL	GBR	FIN	CHE	QAT	LBN
Is an initial outage report required?	✓	✓	✓	✓	✓	✓	✓	✓	✓
Time of submission of the initial outage report	Not defined	Within 1h	Within 2h	Within 0.5-2h	Within 3-72h	Within 1-24h	ASAP[4]	Within 2h	ASAP
Are update notifications required?	✓	✓	✗	✓	✗	✓	✓	✓	✗
Periodicity of updates	Not defined	Every 4h	N/A	Every 1h	N/A	Every 3-12h	Every 2-24h	Every 4h	N/A
Is resolution notification required?	✓	✓	✗	✗	✗	✓	✓	✗	✓
Time of submission of the resolution notification	Within 24h after resol.	Within 1h after resol.	N/A	N/A	N/A	ASAP	Within 2h after resol.	N/A	ASAP-7d
Is a final outage report required?	✓	✓	✓	✓	✗	✓	✓	✓	✗

[3] Ranges mean that different times of submission are applied to different categories of outages.

[4] As soon as possible.

Reporting stage[3]	JAM	CYM	DOM	CHL	GBR	FIN	CHE	QAT	LBN
Time of submission of the final outage report	Within 48h after resol.	Within 14d after resol.	Within 24h after resol.	Not defined	N/A	Within 7d after detec.	NRA discretion	5d after detec.	N/A

Exhibit 6: International benchmark study regarding reporting processes [Source: Axon]

3.3.10 Most benchmark countries define three (3) notification stages, namely "*initial outage notification*" (upon detection), periodical "*update notifications*" as long as the outage persists, and final "*outage report*", upon resolution. One-half of them also define a "*notification of resolution*" of an outage.

3.3.11 As regards to service providers in Jamaica, the procedure involves the four (4) stages presented above whenever the OUR is informed of outages.

3.3.12 The timeframes to submit each notification/report differ among countries. In some countries, the deadline to submit the notification/report also depends on the category of the outage.

3.3.13 Except for the Dominican Republic, all the benchmark countries define the information that service operators must provide about outages in each stage. The countries are well-aligned on the information to be reported, and they all require more details as the outage resolution process advances. Exhibit 7 presents a summary of the key information that service providers must provide in each jurisdiction, and the time at which such information is typically required.

Information	JAM	CYM	DOM	CHL	GBR	FIN	CHE	QAT	LBN
Licensee's contact details	✓	✓	N/A	✓	✓	✓	✓	✗	✓
Date and time of the outage detection	✓	✓	N/A	✓	✓	✓	✓	✗	✓
Description of the outage	✓	✓	N/A	✓	✓	✓	✓	✗	✓
Fault status	✗	✗	N/A	✗	✗	✗	✓	✗	✓
Geographical area affected	✗	✓	N/A	✓	✓	✓	✓	✓	✓
Network assets and services affected	✗	✗	N/A	✓	✓	✓	✓	✓	✓
Number of users affected	✓	✓	N/A	✓	✓	✓	✓	✗	✗
Time of restoration	✓	✓	N/A	✓	✗	✓	✗	✓	✓

Information	JAM	CYM	DOM	CHL	GBR	FIN	CHE	QAT	LBN
Corrective measures applied	✓	✓	N/A	✓	✓	✓	✓	✓	✓
Root-cause analysis	✓	✗	N/A	✓	✓	✓	✓	✗	✓
Actions to prevent future outages	✗	✗	N/A	✓	✓	✓	✓	✗	✗

Initial notification + update notification + resolution + outage report

Exhibit 7: International benchmark study regarding reporting forms [Source: Axon]

3.3.14 In general, initial notifications promote speed over information completeness, and leave information about the diagnosis and the impact of the outage to the update notifications. Resolution reports confirm the restoration of services and provide information about any corrective measure(s) taken to restore the normal functioning of network and services, whereas RCA and details on any risk mitigation actions adopted by the telecommunications service provider are not provided until the final outage report.

Sanctions

3.3.15 None of the benchmark countries define specific sanctions/penalties for non-compliance with the provisions outlined in their outage protocols. However, the outage protocols of half of the countries in the benchmark, particularly the Caribbean and Latin American countries (as shown in Exhibit 8), make reference to the general provisions on sanction/penalties in the corresponding telecommunications/ICT legislations.

Area	JAM	CYM	DOM	CHL	GBR	FIN	CHE	QAT	LBN
Are any sanction or penalty mentioned in the outage protocol?	N/A	✓	✓	✓	✗	✗	✗	✗	✓
Where mentioned are there specific sanctions/penalties defined?	N/A	✗	✗	✗	N/A	N/A	N/A	N/A	✗
If "not", where are they defined?	N/A	Sec 58 of ICT Law	Art 30 of Ley Telec.	Title VII of the Act	N/A	N/A	N/A	N/A	Not defined

Exhibit 8: International benchmark review regarding sanctions [Source: Axon]

Resiliency measures

National Roaming in Emergency Situations

3.3.16 Millions of citizens worldwide rely on their telecommunications services for work, social life, leisure, and to access various public services and different types of assistance. In the case of emergency situations such as disasters, the security and stability of telecommunication networks is of crucial importance for the security of life and property of citizens.

3.3.17 In 2013, the European Union Agency for Cybersecurity (then the European Union Agency for Network and Information Security (ENISA) issued a report entitled "National Roaming for Resilience". In that report, ENISA noted that given the reliance of European citizens on mobile telephony for work, social life and in time of emergencies, outages on a mobile network can have a severe impact on both the economy and the society. ENISA recommended that EU Member States initiate a "*discussion of national roaming as a resilience solution with the mobile telecom operators in order to develop schemes to mitigate large outages*…"[5]

3.3.18 In some countries, like the Maldives, Bahamas, or Sweden, national roaming agreements between mobile service operators are mandatory in disaster response and recovery. Users of a mobile operator facing a network outage during the first phases of a disaster may use any available network including those of the other operators. In Sweden, such national roaming is allowed for a limited number of SIM cards (called emergency SIMs cards) which are distributed to specific crisis centres and the use of these cards are restricted to activities designated by the NRA. This limits the traffic load transferred to the host network.

3.3.19 In the Netherlands, operators voluntarily reached an agreement for national roaming during discussions fostered by the NRA after a huge outage in 2012. National roaming can be activated at the regional level if there is a major outage

[5] https://www.enisa.europa.eu/publications/national-roaming-for-resilience

in the network of one operator, which affects more than 500k users and is expected to last for more than three days. In this situation, two (2) operators would handle the traffic of the third operator experiencing the major outage. End-users of the impacted operator would need to manually select the network on which they want to roam. The costs for traffic handling during the activation period are based on the European roaming tariffs[6].

3.3.20 Similar voluntary agreements were signed by AT&T and T-Mobile in the USA after hurricane Sandy in 2012[7]. In the British Virgin Islands, CCT and Digicel also facilitated emergency roaming between their networks in 2013[8].

3.3.21 National roaming agreements may also be helpful in the completion of emergency calls. In the UK, when a mobile phone is used to make a call to any emergency number and the network of the caller's provider is unavailable, the call will roam onto an alternative network that has the best signal in the area (see Guidance on Telecoms Resilience, last updated in Dec 2019).

Disaster Plans/Business Continuity Plans

3.3.22 The International Telecommunication Union's "*Guidelines for National Emergency Telecommunication Plans*"[9], emphasise the importance of network contingency plans for when emergencies/disasters occur. The ITU noted that response and contingency plans, "*will set an environment to support the continued operation and restoration of communications, which enables timely, effective, and appropriate responses to disasters*". The Guidelines state that *"it is important that all*

[6] See details in ENISA's "National Roaming for Resilience" report at https://www.virginislandsnewsonline.com/domains/virginislandsnewsonline.com/en/news/update-ccts-gsm-network-fully-restored , last accessed on April 2022

[7] Berry Review (2012), AT&T & T-Mobile Enter Into Emergency Roaming Agreement for Hurricane Sandy, see at http://www.berryreview.com/2012/10/31/att-t-mobile-enter-into-emergency-roaming-agreement-for-hurricane-sandy / last viewed on April 2022

[8] Supra note 6

[9] https://www.itu.int/en/ITU-D/Emergency-Telecommunications/Pages/Publications/Guidelines-for-NETPs.aspx

stakeholders have their own standard operating procedures (SOPs) for the different types of emergencies and that these are aligned with the national emergency telecommunications plan and national coordinating mechanisms".

3.3.23 In response to the RFI process launched in November 2021, four (4) of the seven (7) operators confirmed that they already have disaster management plans in place. Of the three (3) operators who stated that they did not have a disaster plan, one mentioned that such issues were addressed in weekly meetings while another indicated that it was in the process of developing such a plan.

3.3.24 In the Bahamas, the Utilities Regulation and Competition Authority requires critical electronic communication infrastructure providers to "*develop and implement procedures to improve Disaster Preparedness to enhance the resilience of its networks against potential threats*".[10] Such plans must be updated every three years. A similar approach is being proposed in Trinidad and Tobago. In its "*Consultative Document on the National Emergency Communications Plan*", the Telecommunications Authority of Trinidad and Tobago (TATT) has proposed that all network operators be required to conduct risk analyses and develop disaster preparedness and business continuity plans. Network operators would be required to update these elements regularly, and make them available to TATT on an annual basis for review and comments.

3.3.25 Business continuity plans are often mandatory for telecommunications service providers in response to a particular hazard. For instance in the Philippines, such plans were required for managing the COVID-19 pandemic[11].

3.4. Key takeaways

3.4.1 The key takeaways from the international comparison are summarised below:

[10]https://www.urcabahamas.bs/publications/ecs-18-2020-disaster-management-regulations-for-the-electronic-communications-sector-in-the-bahamas/

[11] See https://ntc.gov.ph/wp-content/uploads/2020/05/MO-BCP-04-06-20.pdf

- Benchmark countries define a tiered categorisation of outages, based on their scope and impact.
- The process of notifying the relevant authority of outages, and the means of such communication are usually included in the protocols. Provisions regarding notifications to the public are also included.
- Outages are reported to the relevant authority following a stage-by-stage process aiming to provide the authority with comprehensive insights on the outage. The manner in which the outage is categorised helps to define the process.
- Minimum information requirements for every stage are defined in the protocol so as:
    i. to keep authorities informed;
    ii. to allow authorities to understand and evaluate the severity of an outage; and
    iii. to standardise the format of outage reports among service providers.
- The minimum information requirement increases for every successive report that the Licensee submits to the regulatory authority, as the Licensee's technical team can progressively identify and understand the reasons and scope of the outage.
    - Initial notifications simply require the Licensee's contact details, date and time of the onset of the outage, its description, and the geographical area and networks affected.
    - Updates require more details about the outage, an estimation of its duration, as well as a more accurate description of its scope.
    - Resolution notifications usually require the time of restoration of the affected network elements or services, and details about the corrective actions taken.
    - Most of the countries require, in the final outage report, a root-cause analysis and the list of actions taken or to be taken by the Licensee to prevent future similar outages.
- Some countries use national roaming agreements to improve the resiliency of mobile networks, and ensure emergency communication continuity.
- Some jurisdictions require their telecommunications operators to prepare and update periodically, disaster response and business continuity plans.

Chapter 4. Outage Reporting Protocol

4.1.1 This chapter provides information on the proposed outage reporting protocols and resiliency measures in light of best practices identified in the international benchmark review. In particular, it provides information on the OUR's proposals regarding the following key topics:

- Section 4.1. Categories of outages, the categories of outages defined in the draft Protocol.
- Section 4.2. Designation of contact persons, the designation of a contact person in charge of reporting outages to the relevant authority.
- Section 4.3. Reportable outages, the notification stages to be followed by service providers in the event of an outage.
- Section 4.4. Reporting formats, the content of the reports to be submitted by service providers when reporting an outage.
- Section 4.5. Notification to end-users, the communication of outages to the end-users.
- Section 4.6. Draft Outage Reporting Protocol, the reference to the draft Protocol.
- Section 4.6. Resiliency measures

4.1. Categories of outages

4.1.1 The draft Protocol relies on two (2) different sets of criteria to classify outages. The first is based on whether the outage is planned or unplanned; while the other classifies outages (both planned and unplanned) based on their severity.

Planned and unplanned outages

4.1.2 The draft Protocol distinguishes between the management of "*planned*" outages (e.g., service interruptions caused by regular operation and maintenance activities) and "*unplanned*" outages. This is consistent with the "*General Consumer Code of Practice for the Telecommunications Industry"* (hereinafter, "GCCP"), September 2016. This document sets out the basic/standard practices that the OUR recommends that Licensees undertake in service provisioning. In particular, the draft Protocol develops on paragraph 15.1 of the GCCP which states that "[L]*icensees should give advance warning of anticipated service disruptions or planned outages*".

4.1.3 The GCCP however does not specify any timeframe for the advance notice of a planned outage. In reviewing the benchmark references, the Dominican Republic, Finland, and Qatar include specific provisions for such outages; however, only Qatar clearly defines a minimum period of 48 hours of advance notice to provide notification on a planned outage. The OUR has reviewed other international references outside the benchmark countries specified in section 3.3. In particular, the OUR has reviewed the provisions of ECTEL's member states and found that, in their current QoS regulatory framework (approved by all member states except St. Vincent and The Grenadines), the advance notice is also set to 48 hours.[12]

4.1.4 Considering the foregoing assessment, the OUR is of the view that planned outages must be communicated to the OUR and to the public in general, at least two (2) working days (i.e., 48 hours) in advance.

Question 1: Do you consider reasonable the proposed minimum time to notify planned outages in advance? Please support your answer and any suggestions with relevant information and internal or international best-practice references.

Categorisation of outages based on severity

4.1.5 Benchmark countries and service providers in Jamaica as a common practice, utilise a number of factors to determine severity.

4.1.6 Jamaican service providers typically classify outages in two (2) to four (4) categories, based on the severity and scope of the outage (e.g., by using the number of nodes, number of users, or services affected), and/or the nature of the outage.

4.1.7 As indicated in section 3.3, the international benchmark shows a similar pattern in terms of the number of outage categories. In particular:

- Three countries (the Dominican Republic, Switzerland, and Qatar) just define conditions for "reportable" and "non-reportable" outages.

[12] Source: St. Christopher and Nevis, "Telecommunications (Quality of Service) Regulations", 2008; Available at: Link. Please note that this is the current regulation approved in St. Christopher and Nevis, but identical regulations are approved in the remaining member states.

- ▶ The remaining countries go beyond whether the outage is reportable or not and define different reportable categories, based on the scope and impact of the outage. More precisely,
  - Four (4) countries (Cayman, Chile, United Kingdom, and Lebanon) define three (3) categories.
  - One (1) country (Finland) defines four (4) categories.

4.1.8 The OUR is of the opinion that a more granular categorisation of outages may force Licensees to better evaluate and communicate the scope and impact of the outage, allow for adjustments to the notification procedure, and generally contribute to a better handling of outages. Furthermore, some Jamaican operators are used to defining more than two (2) categories of outages, which is aligned with the approach followed by Chile, Lebanon, Cayman, and Finland.

4.1.9 Consequently, the OUR is of the view that a three-tier categorisation provides sufficient granularity without significantly increasing the complexity of the process. Ranked from high to low, the three (3) outage categories proposed are critical, major, and minor.

Question 2: Do you find the number of outage categories reasonable? Please support your answer and any suggestions with relevant information and internal or international best-practice references.

4.1.10 The impact and scope of outages are used to determine their category of severity. Although disparate criteria are used among benchmark countries, all countries except for Lebanon categorise outages based on the number of users affected. Two (2) of the eight (8) benchmark countries rely on the affected level of the network (i.e. core or access), while two (2) countries categorise outages based on the number of access nodes and sites affected. In addition, half of the countries surveyed consider a degradation of emergency communications and/or critical or special infrastructures (where core equipment is also involved).

4.1.11 The OUR is of the view that criteria such as the affected network level (i.e. access or core), the number of access nodes or sites, the type of communication services or infrastructure affected (i.e. emergency services and/or critical or special infrastructures), as an outage affecting these elements may severely affect the wellbeing of citizens and key services for the country's security. Additionally, the number of affected users must also be considered to determine the severity of an

outage. Further, from the responses received in relation to the RFI, Licensees use the affected level of the network, and the number of access nodes and sites affected as a part of the assessment of the severity of an outage. It is the OUR's view that given that service providers have indicated that they are currently using these elements to assess the severity of the outage, such information should be readily available to be used in the categorisation process of the draft protocol.

4.1.12 Based on the foregoing, the following categorisation and criteria are being proposed:

- A critical outage is an outage: i) affecting the users' ability to access emergency services, ii) affecting critical or special facilities, iii) affecting the core network, iv) affecting more than 100 telecommunication access nodes or sites, or v) affecting more than 20% of the Licensee's customer base for the affected service or more than 100k users in different parishes.
- A major outage is an outage that has an impact on the performance of 10 or more access nodes or sites or affects more than 5% of the Licensee's customer base for the affected service or more than 20k users.
- A minor outage is any outage that is not deemed critical nor major.

Question 3: Do you find the categorisation criteria and specific thresholds used reasonable? Please support your answer and any suggestions with relevant information and internal or international best-practice references.

4.2. Designation of contact persons

4.2.1 Some of the benchmark countries (Cayman Islands, Chile, United Kingdom, and Finland) require the designation of a contact person responsible for reporting outages to the relevant authority. The OUR is of the view that designating a contact person facilitates the appropriate communication channel between the service provider and the relevant authority in regard to the outage.

4.2.2 Accordingly, the draft Protocol includes provisions that require service providers to designate a contact person within their organisation to report outages to the relevant authority. In addition, specific contact persons may be identified in an Initial Outage Notification and in subsequent periodic reports.

Question 4: Do you find it reasonable to designate a contact person who reports outages to the relevant authority? Please support your answer and any suggestions with relevant information and internal or international best-practice references.

4.3. Reportable outages

4.3.1 A first step in the categorisation of an outage is to determine whether an outage must be reported to the relevant authority.

4.3.2 In line with the GCCP, the OUR is proposing that all planned outages to be reported.

4.3.3 Regarding unplanned outages, all the countries examined except Lebanon show that service providers are not required to report all unplanned outages on their network, as reporting those with very little impact on the service provisioning (e.g., the shut-down of a sector of a base station) would generate a disproportionate reporting burden for service providers. Consequently, the draft Protocol considers that only outages categorised as "*major*" and "*critical*" are required to be reported, although service providers are encouraged to report minor outages.

Question 5: Do you find the proposal that all planned outages, and critical and major unplanned outages should be reported reasonable? Please support your answer and any suggestions with relevant information and internal or international best-practice references.

4.3.4 Benchmark countries usually follow a multi-step process when reporting an outage. In particular:

- all benchmark countries consider it necessary for service providers to initially notify the relevant authority of the occurrence of the outage;
- five (5) of the eight (8) benchmark countries deem it appropriate for service providers to send update notifications to the relevant authority, on the status of the outage;
- four (4) benchmark countries require service providers to notify the clearance of the outage; and
- six (6) benchmark countries require service providers to complete a comprehensive final report.

4.3.5 In line with international best practice, the draft Protocol considers the following four (4) reporting stages:

- An Initial Outage Notification must be submitted within one (1) hour upon detecting a major or critical unplanned outage.
- Outage Update Notifications must be submitted every hour in the case of critical unplanned outages and every two (2) hours in the case of major unplanned outages.
- An Outage Resolution Notification must be submitted within one (1) hour after the resumption of the normal functioning of the network. In the case of critical outage, service providers must notify the OUR immediately after the restoration.
- An Outage Report must be submitted to the OUR no later than fourteen (14) days after the outage resolution notification.

Question 6: Do you find the four-step reporting process defined in the draft Protocol and its timeframes reasonable? Please support your answer and any suggestions with relevant information and internal or international best-practice references.

4.4. Reporting formats

4.4.1 Service providers must provide accurate complete information about the outage to the relevant authority at each notification stage. Exhibit 7 provides the minimum information that each benchmark country requires service providers to report at each notification stage. In particular:

- The minimum required information requested in the majority of jurisdictions for the Initial Outage Notification is: i) contact details of the service provider, ii) date and time of the onset of the outage, iii) description of the outage, iv) geographical area(s) affected, v) network elements affected, and vi) services affected.

  The OUR is of the view that service providers in notifying that an outage has occurred should be required to provide similar information as that required by majority of the benchmark countries. Further, the OUR is of the view that the Initial Outage Notification should also include preliminary information on the reasons that caused the outage, as this will benefit the management of the event.
- In the case of Outage Update Notifications, in addition to the information in the Initial Outage Notification, the majority of jurisdictions require the inclusion of the number of users affected. Given that more information would be available, service providers must provide information on the number of users affected as

well as, through periodic notifications, and their best estimates on the time required to resolve the outage.

- For Outage Resolution Notification, in addition to the information in the Outage Update Notification, the benchmark countries require service providers to provide the actual time of restoration, as well as the corrective measures applied to clear the outage. The OUR proposes that similar information be required from the service providers.
- Outage Reports usually include, in addition to more details on the previous information reported, a root-cause analysis of the outage and a list of preventive actions taken or to be taken by Licensees to avoid the recurrence of similar outages. In addition to the foregoing, the OUR proposes that service providers include a comprehensive report on the course of events from the detection of the outage up to its resolution, including how it was detected.

Question 7: Do you find the information required at each stage of the notification process reasonable? Please support your answer and any suggestions with relevant information and internal or international best-practice references.

4.5. Notification to end-users

4.5.1 In addition to any reports to the relevant authority, benchmark countries require that end-users be notified of any planned or unplanned outages if certain conditions are met. In fact, the notification of planned outages to end-users is included by the GCCP.

4.5.2 In the case of unplanned outages, the OUR has found, by analysing the operators' responses to the RFI, that it is common practice among Jamaican service providers to notify end-users of outages that have occurred. In particular, two (2) operators clearly state that end-users are notified in case of major or critical outages.

4.5.3 Three benchmark countries (the Dominican Republic, Finland, and Qatar) require that service providers notify end users of unplanned outages, under certain conditions:

- In the Dominican Republic, end-users must be notified for any outage deemed Type 2.
- In Finland, end-users are notified when an outage i) lasts for more than 60 minutes and ii) affects more than 250 users. Nonetheless, if the outage lasts for

more than one (1) week, end-users are notified regardless of the number of them that is affected.

- In Qatar, end-users are notified for any notifiable outage.

4.5.4 It is clear from the above that service providers are not required to notify end-users of all unplanned outages occurring on their network. In line with international best practice, the OUR is of the view that only critical and major outages must be notified to end-users.

4.5.5 The draft Protocol proposes that service providers must notify end-users about any planned outage and any major or critical unplanned outage, through relevant mainstream communication channels accessible by a large segment of the population.

Question 8: Do you find it reasonable to notify end-users about any planned outages, and any major or critical unplanned outage? Please support your answer and any suggestions with relevant information and internal or international best-practice references.

4.6. Draft Outage Reporting Protocol

4.6.1 Please refer to Annex A for the proposed Outage Reporting Protocol, which has been drafted taking into consideration international best practice.

Question 9: Do you have any other comments on the proposed Outage Notification Protocol which have not been discussed previously? Please support your answer and any suggestions with relevant information and internal or international best-practice references.

4.7. Resiliency Measures

National Roaming during Disasters

4.7.1 During emergency situations such as disasters, the security and stability of telecommunication networks is of crucial importance for the security of life and property of citizens. As noted in the previous chapter, reciprocal national roaming agreements between mobile network operators can help strengthen the resiliency of telecommunication networks in disaster situations. The OUR is cognizant that significant effort will be required to conclude the technical and commercial aspects

of such agreements including the scope of roaming services to avoid overloading the host network and the terms and conditions[13]. However, the OUR is of the view that given the vital importance of telecommunications during the response and recovery of a disaster, it is essential that initiatives such as national roaming be explored to ensure the continuity of communications in emergency situations.

4.7.2 The OUR is therefore considering the inclusion of the following provisions in the Outage Reporting Protocols and Measures to Improve Network Resiliency in Disasters found in Annex A:

4.7.2.1. All mobile voice service providers shall negotiate, conclude and implement a national roaming agreement that enables the activation of a national roaming service, on a reciprocal basis, as soon as the designated government agency issues a warning of an impending national emergency or national disaster, and for the whole duration of such national emergency or national disaster. All such national roaming agreements shall be submitted to the Office for its approval, within six (6) months of the publication of these Protocols.

4.7.2.2. Mobile voice service providers shall duly inform the Office of a decision to activate or de-activate national roaming in parts or all of the areas impacted by the national emergency or national disaster under the terms of this national roaming agreement.

4.7.2.3. The Office reserves the right to decide whether it is in the public interest that roaming services should be activated or de-activated during a national emergency or national disaster, and may therefore require the operators to activate or de-activate roaming services accordingly.

Question 10: Do you think the proposal to include national roaming obligations in cases of disasters is reasonable? Please support your answer and any suggestions with relevant information and internal or international best-practice references.

Emergency Mobile Roaming

4.7.3 Currently, in Jamaica mobile calls to emergency numbers can only be connected if the caller's own network is available in the area. This can be an issue given that coverage issues persist in some areas. The OUR has found that some countries are requiring mobile service operators to conclude national roaming agreements that let users make calls to emergency services using the network of other mobile network operators when the network of their provider is unavailable.

4.7.4 The OUR is of the view that ensuring mobile users have backup coverage when out of range of their own network will improve safety during emergency situations. The OUR is therefore proposing to include the following provision regarding emergency calls in the Outage Reporting Protocols and Measures to Improve Network Resiliency in Disasters in Annex A:

4.7.4.1. Mobile voice service providers shall negotiate, conclude and implement agreements that enable users to call the national pre-defined emergency numbers from another network if the network of their service provider is unavailable and the area concerned is covered by another network. Such agreements must be submitted to the Office for its approval, within six (6) months of the publication of these Protocols.

Question 11: Do you think the proposed obligation to extend the accessibility of emergency services by enabling users wishing to call an emergency number to roam on any other available network if their own service provider's network is unavailable reasonable? Please support your answer and any suggestions with relevant information and internal or international best-practice references.

Disaster plans/Business continuity plans

4.7.5 As outlined earlier, in some jurisdictions telecommunications operators are required to prepare and submit to the NRA, plans which outline how they will respond in instances of emergencies/disasters including steps that will be taken to facilitate the restoration of telecommunications services impacted by an

emergency/disaster. The OUR is of the view that in order to ensure continuity of telecommunications services before, during, and in the aftermath of disasters, it is necessary to have the appropriate plans which outline the agreed policies, procedures and processes which will be triggered in cases of emergencies/disasters.

4.7.6 The review of the responses to the RFI issued on 2021 November 2, found that not all telecommunications service providers have disaster plans in place. The OUR is therefore proposing for inclusion in the Outage Reporting Protocols and Measures to Improve Network Resiliency in Disasters, provisions related to the submission of Disaster and Business Continuity Plans by Licensees to the Office. The proposed provisions are as follows:

4.7.6.1. Licensees shall conduct an annual risk analysis of their critical facilities, in accordance with their established internal audit procedures, and take measures to reduce their network vulnerability.

4.7.6.2. Licensees shall, within three (3) months after the publication of these Protocols, develop and implement procedures to enhance the resilience of their networks and ensure the proper and effective functioning of these networks at all times during all phases of a disaster or an emergency. These procedures should be outlined in the Licensees' disaster preparedness and business continuity plans which shall be submitted to the Office for approval.

4.7.6.3. The disaster preparedness and business continuity plans shall be updated and resubmitted to the Office at least once every two (2) years.

Question 12: Do you find the proposed provisions regarding the development, implementation, submission and updates of Disaster Plans and Business Continuity Plans reasonable? Please support your answer with relevant information and internal or international best-practice references.

Chapter 5. Summary of questions

5.1.1 **Question 1:** Do you consider reasonable the proposed minimum time to notify planned outages in advance?

5.1.2 **Question 2:** Do you find the number of outage categories reasonable?

5.1.3 **Question 3:** Do you find the categorisation criteria and specific thresholds used reasonable?

5.1.4 **Question 4**: Do you find it reasonable to designate a contact person who reports outages to the relevant authority?

5.1.5 **Question 5**: Do you find the proposal that all planned outages, and critical and major unplanned outages should be reported reasonable?

5.1.6 **Question 6**: Do you find the four-step reporting process defined in the draft Protocol and its timeframes reasonable?

5.1.7 **Question 7**: Do you find the information required at each stage of the notification process reasonable?

5.1.8 **Question 8**: Do you find it reasonable to notify end-users about any planned outages, and any major or critical unplanned outage?

5.1.9 **Question 9**: Do you have any other comments on the proposed Outage Notification Protocol which have not been discussed previously?

5.1.10 **Question 10**: Do you think the proposal to include national roaming obligations in cases of disasters is reasonable?

5.1.11 **Question 11**: Do you think the proposed obligation to extend the accessibility of emergency services by enabling users wishing to call an emergency number to roam on any other available network if their own service provider's network is unavailable reasonable?

Question 12: Do you find the proposed provisions regarding the development, implementation, submission and updates of Disaster Plans and Business Continuity Plans reasonable? Please support your answer with relevant information and internal or international best-practice references.

Annex A. Draft Outage Reporting Protocol and Measures to Improve Network Resiliency in Disasters

The Outage Reporting Protocols and Measures to Improve Network Resiliency in Disasters

Part I. Introduction

1 Short title

1.1. These Outage Protocols and Network Resiliency Measures in Disasters may be cited as the Outage Reporting Protocols and Network Resiliency Measures, 2022.

2 Scope and objectives

2.1. The Office of Utilities Regulation (hereinafter, "the Office"), in exercise of the powers vested in it by the Telecommunications Act, hereby establishes the requirements pertinent to the reporting of outages to telecommunication services or any incident that threatens the reliability and the security of telecommunications infrastructure/facilities, and network resiliency measures (henceforth, "the Protocols and Resiliency Measures").

2.2. The objectives of these Protocols and Resiliency Measures are to ensure that–

a) the Office is properly informed, in a timely manner, of any relevant disruption in telecommunication services and the steps being taken to restore service;

b) a proper assessment of disruptions is undertaken and appropriate corrective actions are taken to prevent a recurrence of a disruption of a similar nature;

c) end-users are informed of any Planned and /or Unplanned Outages;

d) there is continuity or quick recovery of operations in cases of emergency situations or disasters.

2.3. These Protocols and Resiliency Measures shall apply to all Licensees.

Part II. Interpretation

3 Interpretation

3.1. In these Protocols and Resiliency Measures, unless the context otherwise provides –

a) "Act" means the Telecommunications Act.

b) "Core Network" means the highest level in a network's architecture, which is in charge of connecting remote access nodes, and hosting service and network platforms that are critical for the proper provision of telecommunication services, and whose malfunction will affect a significant share of the users of the network.

c) "Critical or Special Facilities" means any telecommunications facilities that have been designated as such by the Office.

d) "Emergency Services" means services offering consumers the ability to connect in priority, from any service area via any subscriber or public terminal or device, to national pre-defined emergency numbers to communicate any emergency situation, regardless of the consumer's subscription status.

e) "Licensee" has the same meaning as in the Act.

f) "Outage" means a degradation in the ability of an end user to establish and/or maintain a channel of communication as a result of the failure of, or degradation in the performance of, a Licensee's network or service.

g) "Planned Outages" are outages of a Licensee´s telecommunications network that are part of regular operation and maintenance activities, where the Licensee (i) knows at least seventy-two (72) hours in advance that such an event will occur and (ii) has notified the Office and all affected end-users that the Outage will occur.

h) "Unplanned Outages" are any outages that cannot be considered a Planned Outage.

Part III. Categorisation of Outages

4 Categorisation of outages

4.1. Critical Outages are defined as those

(1) affecting users' ability to access Emergency Services, or

(2) affecting Critical or Special Facilities, or

(3) affecting the Core Network, or

(4) affecting more than 100 telecommunication access nodes or sites, or

(5) affecting more than 20% of the Licensee's customer base for the affected service or more than 100k users in different parishes.

4.2. Major Outages are defined as those that

(1) have an impact on the performance of 10 or more access nodes or sites, or

(2) affect more than 5% of the Licensee's customer base for the affected service or more than 20k users.

4.3. Minor Outages are defined as any outages other than Critical or Major Outages.

Part IV. Outage notification process

5 Designation of contact persons

5.1. Licensees shall designate a person in charge of submitting Outage notifications and reports to the Office (the "Contact Person"), and shall provide the Office with the person's contact information. The Contact Person shall have responsibility for the completeness and accuracy of the information contained in the Outage notifications and reports.

5.2. The Contact Person shall certify and sign the notifications and Outage reports prior to submitting them, and ensure that the information contained therein is complete and accurate to the best of his/her knowledge and belief.

5.3. Licensees shall promptly notify the Office of any changes in the Contact Person's identity or contact details.

5.4. Licensees may designate other specific Contact Persons in each Outage notification. Should the Office require further information about an Outage, the Office may contact the specific Contact Person for that Outage notification, if that Contact

Person is specified in the last notification about that Outage, and/or the default Contact Person designated by the Licensee.

6 Outage notification process

6.1. A Licensee shall give its customers and the Office two (2) working days advanced notice of any period of Planned Outages that is scheduled for routine maintenance or for upgrading of its network.

6.2. The notice to the Office shall include details of the nature of the maintenance or the upgrading of the network and the estimated duration of the Planned Outage. Where a Planned Outage exceeds the estimated duration, it shall be considered as Unplanned from the initial estimated time for the service and network to be restored. The Licensee shall notify the Office, as soon as practicable after becoming aware that the Outage is likely to exceed the estimated duration and provide reason(s) for the delay and a new estimated time for restoration of service.

6.3. Licensees shall report to the Office any Major or Critical Unplanned Outage.

6.4. Within one (1) hour upon detecting a Major or Critical Unplanned Outage, the Licensee shall submit an Initial Outage Notification of any such Outage to the Office.

6.5. In the event of an Unplanned Critical Outage lasting more than one (1) hour, the Licensee shall submit periodic Outage Update Notifications every hour, until the resolution of the Unplanned Critical Outage. For Unplanned Major Outages, lasting more than two (2) hours, the Licensee shall submit an Outage Update Notification to the Office on the 2nd hour and periodic Outage Update Notifications every two (2) hours thereafter, until the resolution of the Unplanned Major Outage.

6.6. Licensees shall notify the Office of the resolution of any Unplanned Critical Outage immediately after the normal functioning of the communication networks and /or services has been restored. Within one (1) hour of said restoration, the Licensee shall submit an Outage Resolution Notification to the Office. Regarding an Unplanned Major Outage, the Outage Resolution Notification shall be made by the Licensee to the Office no later than one (1) hour after the normal functioning of the communication networks and /or services has been restored.

6.7. Licensees shall submit to the Office a detailed Outage Report no later than fourteen (14) days after the Outage Resolution Notification.

7 Means of communication

7.1. Outage Notifications and reports shall be submitted to the Office via e-mail to the contact person designated by the Office to handle such matters or through any other electronic platform so designated.

7.2. In the case of Critical Outages, the Initial Outage Notification shall be made by telephone to the contact person so designated by the Office, in addition to the aforementioned means of notification.

8 Content of the Outage notification reports

8.1. The Initial Outage Notification shall be provided according to the template in Appendix A.1, and shall contain the following information:

a) Licensee Name

b) Date and time of the onset of the Outage

c) Category of the Outage

d) Geographical area(s) affected

e) Network elements affected

f) Telecommunication services affected

g) Description of the Outage, including any additional relevant details (e.g., how it was detected, and its effect on the affected users or services)

h) Contact details of the technician or other persons whom the Office may contact, for the purpose of requesting additional information, if different from the default Contact Person designated by the Licensee.

i) A short description of the reason(s) that caused the Outage if known to the Licensee at the time of issuing the notification.

8.2. Outage Update Notifications shall provide:

a) any update to the information included in the Initial Outage Notification

b) the number of users affected, and

c) the estimated time to resolved the Outage.

d) the estimated time to resolve the Outage.

8.3. The Outage Resolution Notification shall provide:

a) all the information included in the Outage Update Notifications

b) the actual time of restoration, and

c) details on the corrective measures applied.

8.4. The Outage Report shall inform the Office of the detailed root causes of the Outage, and any mitigation actions taken by the Licensee to avoid a future recurrence of the Outage. The report shall include:

a) any update to the information in the Outage Resolution Notification;

b) a comprehensive report on the course of events (i.e., how the disruption was detected, and which corrective measures were taken);

c) a comprehensive root cause analysis according to the principles and guidelines laid out in Appendix 0; and

d) a list of actions taken or to be taken by the Licensee to prevent future similar Outages.

8.5. Planned Outage Notifications shall be submitted according to the template in Appendix A.2, and shall contain the following information:

a) Licensee Name

b) Date and time of the planned Outage

c) Category of the Outage

d) Geographical area(s) to be affected

e) Network elements to be affected

f) Telecommunication services to be affected

g) A description of the Outage and the reasons to schedule it

h) An estimated duration of the Outage

i) Contact details of the technician or persons whom the Office may contact for the purpose of requesting additional information, if different from the default Contact Person designated by the Licensee.

9 Notification to end-users

9.1. Licensees shall notify their customers about any Planned Outage including details on the Outage such as:

a) Its estimated duration; and

b) The services and areas that will be affected;

9.2. Licensees shall notify their customers about any Major or Critical Unplanned Outage including details on the Outage such as:

a) the time of onset of the Outage;

b) the services and areas that are affected; and

c) any applicable compensation or other remedies.

9.3. Such announcements shall be made through relevant mainstream communication channels accessible by a large segment of the population. These may include, without limitation, e-mail, SMS, publication on the Licensee's websites, and communication through social media platforms.

Part V. Resiliency Measures

10 National roaming during disasters

10.1. All mobile voice service providers shall negotiate, conclude and implement a national roaming agreement that enables the activation of a national roaming service, on a reciprocal basis, as soon as the designated government agency issues a warning of an impending national emergency or national disaster, and for the whole duration of such national emergency or national disaster. All such national roaming agreements shall be submitted to the Office for its approval, within six (6) months of the publication of these Protocols.

10.2. Mobile voice service providers shall duly inform the Office of a decision to activate or de-activate national roaming in parts or all of the areas impacted by the national emergency or national disaster under the terms of this national roaming agreement.

10.3. The Office reserves the right to decide whether it is in the public interest that roaming services should be activated or de-activated during a national emergency or national disaster, and may therefore require the operators to activate or de-activate roaming services accordingly.

11 Emergency Mobile Roaming

11.1. Mobile voice service providers shall negotiate, conclude and implement agreements that enable users to call the national pre-defined emergency numbers from another network if the network of their service provider is unavailable and the area concerned is covered by another network. Such agreements must be submitted to the Office for its approval, within six (6) months of the publication of these Protocols.

12 Disaster plans/Business continuity plans

12.1. Licensees shall conduct an annual risk analysis of their critical facilities, in accordance with their established internal audit procedures, and take measures to reduce their network vulnerability.

12.2. Licensees shall, within three (3) months after the publication of these Protocols, develop and implement procedures to enhance the resilience of their networks and ensure the proper and effective functioning of these networks at all times during all phases of a disaster or an emergency. These procedures should be outlined in the Licensees' disaster preparedness and business continuity plans which shall be submitted to the Office for approval.

12.3. The disaster preparedness and business continuity plans shall be updated and resubmitted to the Office at least once every two (2) years.

Part VI. Sanctions

13 Sanctions

13.1. Failure to comply with any provision of these Protocols and Resiliency Measures may result in any of the enforcement actions available to the Office under Part XIII of the Act.

Part VII. Entry into operation

14 Entry into operation

14.1. These Outage Protocols and Resiliency Measures shall come into operation on [XX].

Appendix A Outage Notification Templates

A.1 Unplanned Outage Notification Template

Details of the Licensee		
Name of the Licensee		
Name of the Contact Person in case further information is required by the Office		
Telephone	**E-mail address**	
Minimum information for Initial Outage Notification		
Date and time of the onset of the Outage		
Category of the Outage	☐ Critical	☐ Major ☐ Minor
Geographical area(s) affected		
Network elements affected		
Telecommunication services affected		
Description of the Outage		
Description of the reason(s) that caused the Outage		
Additional information to be included in Outage Update Notifications		
Number of users affected		
Estimated time to resolve the Outage		
Additional information to be included in Outage Resolution Notification		
Actual time of restoration		
Details on corrective measures applied		
Additional information to be included in the final Outage Report		
Course of events		

Comprehensive root cause analysis According to the guidelines provided in 0. Include additional documentation to demonstrate this where necessary
Actions to prevent future Outages

A.2 Planned Outage Notification Template

Details of the Licensee	
Name of the Licensee	
Name of the contact person in case further information is required by the Office	
Telephone	**E-mail address**
Details on the Planned Outage	
Date and time scheduled for the Outage	
Category of the Outage	☐ Critical ☐ Major ☐ Minor
Description of the Outage	
Description of the reason(s) to plan the Outage	
Scope and impact	
Geographical area(s) to be affected	
Network elements to be affected	
Telecommunication services to be affected	
Number of users to be affected	
Estimated duration of the Planned Outage	

Appendix B Root Cause Analysis Methodologies

B.1. A comprehensive and complete root cause analysis ("RCA") must be provided by Licensees in the final Outage Report.

B.2. The RCA must evaluate and analyse the details of the factors that have contributed to causing the Outage. Outages are often due to multiple factors hence the RCA must evaluate a number of them including, but not limited to:

i. the capacity and proper functioning of network elements;

ii. any installation of the most recent updates or versions of software;

iii. the adequacy of existing standard operating procedures or the lack of them;

iv. the presence and proper functioning of backup equipment or infrastructure;

v. any external factors affecting the operation or the network infrastructures.

B.3. Standard RCA methodologies, such as the ones presented in the remainder of this Appendix, may help Licensees conduct a thorough analysis of the factors and situations that contributed to causing the Outage, and identify what measures must be taken to prevent the recurrence of similar Outages in the future.

B.4. A comprehensive RCA must not stop at the first round of apparent reasons for an Outage, but instead include a deeper analysis to identify every contributing factor, its context and its conditions. The "5-Whys analysis" is an iterative RCA technique that aims to identify the root cause of an Outage by repeatedly analysing the factors that contributed to a fault, the reasons that made those factors possible and any measure to prevent similar situations in the future. The "five" in the name suggests a minimum number of iterations that is typically required to arrive at a comprehensive map of the root causes of an Outage. The 5-Whys analysis must be carried out by a competent working group with key management personnel from different departments. The RCA team must undertake subsequent iterations over the following steps:

a) Have a clear picture of the outage (1st *why*) or the cause that contributed to the Outage (subsequent *whys*), and its context.

b) Analyse where, when and how the Outage has occurred and try to identify potential causes (*whys*), and any counter-measure that may prevent it from happening again in the future.

c) For every identified cause, analyse and ask why this caused the Outage.

B.5. The "Fault tree analysis" is a top-down technique in which the possible states of a system are analysed based on the combination of lower-level elements. Its final objective is to identify the most vulnerable part of the system, the core components that ensure its functioning, and the component that caused the maximum number of failures.

B.6. The "Failure modes and effect analysis" is a more complex representation of the fault tree analysis aiming at identifying all potential failures or problems, and ranking them using a risk priority number.

B.7. The "Fishbone diagram" aims at identifying many possible causes for an Outage, and sorting ideas into useful categories. The brainstorming starts by asking "why did the Outage happen?" Factors causing an Outage may be initially classified as follows:

i. Factors related to malfunctions of specific assets (e.g., the network).

ii. Factors related to the processes or methods used to manage the network.

iii. Factors related to manpower or other people playing a role in such processes.

iv. Factors related to demand (e.g., extraordinary traffic spikes, etc.).

v. Lack of measures required to anticipate an Outage or the inadequacy of existing measures.

vi. External factors affecting the operation or the performance of the network (e.g., environmental, changes in the provision of critical inputs from third parties, etc.).

For each cause preliminarily identified, an additional brainstorming must follow. This process is subsequently repeated to detect deeper levels of causes.

"Scatter box diagrams" may be used to detect any correlation between two sets of numerical data. The scatter box diagram is mainly used as a complementary tool when trying to identify the potential root cause of Outages by means of, for instance, fishbone diagrams.