CONSULTATION: DRAFT TELECOMS SECURITY PROCEDURAL GUIDANCE AND RESILIENCE GUIDANCE

SURE (JERSEY) LIMITED CONSULTATION RESPONSE – Non-confidential version

Q1. Do you have any comments on the Authority's role in the telecoms security framework and its approach to issuing Procedural Guidance and Resilience Guidance under the Law?

We support the Jersey Competition and Regulatory Authority ("JCRA") having a role in the Telecoms Security Framework[1]. Indeed, Sure (Jersey) Limited ("Sure") believes that the JCRA should have its role expanded under the Telecoms Security Framework.

As explained in response to Q7 of the Government of Jersey's consultation on the draft Telecommunications (Security Measures) (Jersey) Order 202- ("the Order") and the Telecommunications Security Code of Practice ("the Code"), we contend that the JCRA should be responsible for deciding which electronic communications network and/or service providers ("Providers") should be within scope of the Order and the Code. In our view, the Minister is not well placed to decide which Provider should we within scope for the following reasons:

- **Conflict** – we are concerned that the Government of Jersey's proposed approach could create a conflict for the Minister where, in certain conditions, a Provider may not be included in scope of the Order for political or economic reasons. ✂

- **Procedural complexity** – the process described in the Order and Code of Practice is vague and complex, and likely to take a significant period of time to implement. We have put numerous questions to the Government of Jersey in an attempt to clarify the process, the relevant market share threshold, and the exact mechanism for including Providers in scope[2]. We are happy to share our submission to the Government of Jersey

[1] Together the Telecommunications Law (Jersey) Amendment Regulations 2024, the Telecommunications (Security Measures) (Jersey) Order 202-, and the Code of Practice.

[2] Questions included: Who within Government will keep these market shares under review and how often will such a review take place? Where will this duty be specified so that it is not forgotten or overlooked? Should a change to the Order be required, how long will it take for the Government to produce this change? Will the amended Order need to be consulted on before coming into effect and/or will the amended Order need to be laid before the States Assembly? If a consultation and/or vote by the States Assembly be required, what are the proposed timescales for completing this process (noting that the relevant Provider may have had a significant market share for between two and three years by this point)? Will there be an extraordinary process for amending Schedule 1 of the Order in the event that circumstances require it? Is there a risk that, should an amendment to the Order require States Assembly approval, a particularly busy

with the JCRA should it assist. Notwithstanding our questions above, we are concerned that the Government of Jersey's proposed approach is vague and risks undue complexity and delay in proscribing a Provider as being within scope of the Order and the Code. In our view, this lack of speed and efficiency is sub-optimal and could straightforwardly be avoided if the JCRA was given responsibility for establishing which Providers fall within scope of the Telecom Security Framework based on defined, published criteria.

Given the risk of undue complexity and delay, and the risk that the Minister could find themselves conflicted as to whether to include a specific Provider within scope of the Order and Code of Practice, we have proposed that an alternative approach be taken. We have proposed that the JCRA be responsible for determining which Providers fall within scope and do so on a dynamic basis, reviewing market shares (and other metrics[3]) at intervals which best reflect market developments and without the risk that political and/or economic pressure could unduly influence a decision to proscribe a Provider. We contend that the JCRA is better placed to establish the scope of the Order and Code of Practice, particularly given it produces the statistics which shall be relied on by the Government under its proposals, and therefore we have suggested that the Government of Jersey give this role to the JCRA.

We would like to invite the JCRA to support our proposal to the Government of Jersey. In our view, the process for establishing which Providers fall within scope of the Order and the Code of Practice can and should be set out in this Procedural Guidance. We therefore additionally request that, if agreed to by the Government of Jersey (which in our view, it should), the JCRA should add a new section to this Procedural Guidance which explains the way in which Providers will be included and excluded from scope of the Order and Code of Practice. Specifically, the section should set out:

- The relevant market share threshold and the method through which market shares will be assessed;
- Other metrics which may be indicative of the relevant Provider needing to be included within scope of the Order and Code. For example, we believe that the JCRA should also

parliamentary timetable or an election period may unduly delay the required amendment to the Order? If a Provider is subject to a security duty under the Telecommunications Law (Jersey) Amendment Regulations 2024, but is not subject to the specific measures in the Order, how will the JCRA consider whether the Provider has breached its security duty? Sure's understanding is that it will be unable to rely on either the Order or Code of Practice to demonstrate non-compliance with the security duty under Article 24K.

[3] Sure has proposed to the Government of Jersey that other metrics above and beyond market share be considered when identifying Providers which ought to be in scope of the Order and Code of Practice. This includes considering the financial means of the Provider and whether the Provider has any agreements with providers of critical national infrastructure.

consider whether it is possible for a relevant Provider to afford to comply with the Telecoms Security Framework, irrespective of whether its market share in any given market exceeds the threshold. Similarly, we contend that looking at market share is insufficient to reflect criticality to Jersey and its critical national infrastructure. We therefore believe an additional metric should be whether the Provider has any contractual arrangements with the Government of Jersey and/or providers of critical national infrastructure (Jersey Gas, Jersey Water, Jersey Post, Jersey Electricity Limited etc).

- Any circumstances in which the JCRA may depart from its established mechanism for including/excluding Providers in scope of the Order and the Code.

Q2. Do you have any comments on the Authority's approach to developing its Draft Procedural Guidance and Draft Resilience Guidance?

Sure supports the JCRA's proposed approach to developing its Draft Procedural Guidance. Sure has, however, outlined aspects of the Draft Procedural Guidance which it believes could be better explained, or which should be amended to better suit the Jersey context.

There is no aspect of the Draft Procedural Guidance for which Sure strongly objects.

Q3. Do you agree with the Authority's planned approach to compliance monitoring contained in Section 3 of the Draft Procedural Guidance? If not, please explain why and propose any alternatives.

Sure broadly agrees with the JCRA's planned approach to compliance monitoring for the Telecoms Security Framework. However, we have a number of queries or requests for clarification regarding the proposed approach to compliance monitoring and request that the JCRA provide further information or clarification in its finalised Procedural Guidance.

Firstly, in paragraph 3.11, the JCRA explains that its proposed approach to compliance monitoring will be collaborative and that the JCRA will work with Providers to ensure compliance. Specifically, the Procedural Guidance states that

"where the Authority finds areas of concern, it will seek to work with Providers to ensure appropriate and proportionate measures are implemented in accordance with the telecoms security framework… As necessary, the Authority will also stand ready to engage its suite of enforcement powers with the approach to enforcement."[4]

[4] Draft Telecoms Security Procedural Guidance General statement of policy under Article 24Y of the Telecommunications (Jersey) Law 2002 – page 12, paragraph 3.11

To the extent that we have understood the JCRA's position correctly, we welcome and support this approach. However, the way in which the JCRA's position is currently described in the draft Procedural Guidance does not give much certainty to Providers within scope of the Order. Can the JCRA please set out in more detail/certainty the circumstances in which remedial action via supervision would be adopted and the circumstances in which escalation to more formal enforcement tools would be used?

In our view, the JCRA should follow the approach adopted by the JFSC and other financial services regulators around the world in adopting a 'graduated approach' to supervision and enforcement. This would see the primary/first route to remediating failures be to work with the firm via supervisory engagement to agree on remedial actions and then monitor completion of those actions. Should a particularly serious breach occur, or if persistent failures arise, failure to meet the remediation plan, or a lack of cooperation arises, then the JCRA can move to using more formal enforcement tools.

In our view, this graduated approach will be better suited to driving a positive compliance culture on the topic of security for the following reasons:

- It encourages early engagement and openness (both crucial in dealing with security incidents);
- Supports learning and improvement, over fear of making mistakes;
- Is more proportionate, particularly for smaller organisations like Sure where the cost of compliance is already significant before enforcement action has been taken;
- It encourages senior management and the board to be accountable and generate a positive tone from the top where openness and collaboration with the regulator is prioritised over the desire to cover up security incidents; and
- It recognises that there is a difference between honest mistakes/resource constraints, and misconduct.

We therefore invite the JCRA to clarify its approach to compliance monitoring, collaborative engagement, and enforcement, and specify when it will consider moving from collaborative action to enforcement action. As explained above, we urge the JCRA to mirror the graduated approach taken by financial services regulators and work with Providers to deliver the security outcomes intended by the Telecoms Security Framework.

Secondly, we note that the JCRA intends to begin issuing statutory information requests prior to the first Code of Practice deadline coming into force[5]. We do not object to this approach from the JCRA, and greatly appreciate the JCRA's proposal to structure the issuing of statutory information requests to minimise the burden on Providers. Notwithstanding this, we are

[5] Draft Telecoms Security Procedural Guidance General statement of policy under Article 24Y of the Telecommunications (Jersey) Law 2002 – page 15, paragraph 3.22

confused about how and why the JCRA will be assessing compliance against the Code of Practice prior to the first tranche coming into force, and potentially do the same for future Code of Practice deadlines (bearing in mind the statutory duty and Order security measures will already be in force). With that in mind:

- What approach will the JCRA take to supervision and enforcement in this scenario given that the duty already is in force but the Code of Practice does not yet require compliance with specific measures?
- Is there a risk that a Provider could be found in breach of the duty prior to the first set of security measures coming into force? This is an important point of clarification as Providers will set their compliance/security strategies with the first Code of Practice date in mind.

Please note, Sure and other Providers have requested that the proposed deadlines for Code of Practice be moved back by at least 12 months[6].

Thirdly, in paragraph 3.25, the JCRA explains that it will use "an appropriate platform to securely receive, process and store confidential information"[7].

We welcome the JCRA's confirmation that it will use an appropriately secure platform to store data/information about the secureness of Providers' networks and services. However, given the nature of the information which will be shared by Providers, it is important that we have confidence that this information will be securely stored and not inappropriately accessed. To that end, can the JCRA please provide further information about the systems it will use to securely store confidential information received from Providers?

We understand that the JCRA may not want to publish specific information about its secure systems in this Procedural Guidance. Should that be the case, we would welcome an opportunity to meet with the JCRA to understand the systems and processes it will use to keep Providers' network and service information secure.

Fourthly, we remain concerned about the cost implications for Providers as a consequence of the JCRA's proposed compliance monitoring programme. In paragraph 3.39 of the Procedural Guidance, the JCRA explains that *"Providers have a duty to cooperate with an assessment and are also required to pay the Authority's reasonably incurred costs in connection with the assessment"*.

[6] Sure has requested that the first deadline (31st March 2027) be moved back to 31st March 2028, but has stated that it remains comfortable with the other deadlines.
[7] Draft Telecoms Security Procedural Guidance General statement of policy under Article 24Y of the Telecommunications (Jersey) Law 2002 – page 16, paragraph 3.25

We welcome the JCRA's statements in paragraphs 3.42 and 3.43 in which it suggests assessments and assessment notices will not be used as part of routine compliance monitoring. However, we remain concerned about the cost implications for Providers where assessment notices are used, particularly given some assessments, such as penetration testing, can cost between ✂ per domain[8]. This will particularly be the case if the JCRA, which we recognise has only one Technical Case Officer, decides to use a third party to conduct these assessments. Multiple assessments like this in any given financial year could have a significant cost implication for Sure and other Providers.

We believe a pragmatic alternative approach is possible. Rather than simply issue an assessment notice that could result in a substantial cost to the Provider(s), we propose that the JCRA instead engage in consultation with the relevant Provider(s) to (a) give notice of the use of this assessment notice as part of ongoing compliance monitoring so that the cost can be factored into the budget, and (b) so that there can be discussion about the most cost-effective and efficient approach to fulfilling the assessment notice.

Finally, we would like the JCRA to provide significantly more information about the way in which it intends to use its powers of entry.

Under the Telecommunications Law (Jersey) Amendment Regulations 2024, the JCRA has the power to require entry to a Provider's premises or have the Provider give access to an authorised third party. We recognise and respect this statutory power. However, we don't believe that the JCRA has provided sufficient information or guidance on this topic within the Procedural Guidance and we have some questions about how this will work in practice:

- Will an authorised person be able to access premises without supervision? This would obviously raise its own security concerns and thus we would not be supportive of this proposal (to the extent that it is the case);
- How much notice would the JCRA provide regarding a site visit? Is there the possibility that unannounced site visits could occur and, if so, what arrangements would Providers need to make for such a site visit?
- How will the actions of the authorised person be documented and reviewed during the site visit? If the authorised person is not an employee of the JCRA, what checks will be undertaken to ensure that the authorised person behaves securely and appropriately during the site visit?
- If documents and/or evidence is provided to an authorised person, how will this be securely stored and reviewed?
- If an authorised person is used who is not an employee of the JCRA, can these authorised persons be subject to NDA from the Provider and/or the JCRA so that it is not information which is shared with third parties other than the JCRA?

[8] ✂

The JCRA currently has just two brief paragraphs on this very important topic. We request that the JCRA significantly expand on its explanation regarding when and how it will conduct site visits. In our view, simply stating that "the Authority expects to have regard to any relevant legislation or guidance provided in this area" is insufficient.

Q4. Do you agree with the Authority's planned approach to reporting security compromises contained in Section 4 of the Draft Procedural Guidance? If not, please explain why and propose any alternatives.

Sure broadly supports and agrees with the JCRA's planned approach to reporting a security compromise and significant risks of a security compromise.

The JCRA makes reference to "secure communication methods" in paragraph 4.11 and 4.12[9]. Can the JCRA please set out explicitly which communication methods it considers to be secure?

In paragraph 4.33, the JCRA states that an urgent security compromise should be notified to the JCRA "as soon as possible and usually within 24-hours". The JCRA additionally states that it "then expects the full report to be provided within 72-hours"[10]. We submit that, in many cases, it will be unreasonable and unrealistic to expect a Provider to provide a "full report" regarding the compromise within 72-hours. In Sure's experience, it will be possible to acknowledge awareness of a security compromise, and provide some details of the incident, to the JCRA within 24-hours. It will likely also be possible to provide a more comprehensive explanation of what is known about the security compromise at that time within 72-hours. However, in most cases of a security compromise, particularly in cases of complex cyber security incidents (such as where a state threat actor is involved) or complex network failures, it will take significantly more than 72-hours to thoroughly investigate the incident and complete a full report. Where cases are particularly complex, Sure's experience is that it can take weeks or months to complete the investigation phase of incident repose and then longer to produce a comprehensive report. These timescales will be elongated in complex cases if a third party incident response team is required. It is therefore, in our view, unrealistic to expect a full report to be submitted within the above-mentioned timescales.

[9] Draft Telecoms Security Procedural Guidance General statement of policy under Article 24Y of the Telecommunications (Jersey) Law 2002 – page 24, paragraph 4.11
[10] Draft Telecoms Security Procedural Guidance General statement of policy under Article 24Y of the Telecommunications (Jersey) Law 2002 – page 31, paragraph 4.33

As a result, we request that the JCRA adjust this aspect of the Procedural Guidance. We believe a more pragmatic and proportionate approach would be for the JCRA to require notification of an urgent security compromise within 24-hours, and then receive a further, more detailed (but not full) report within 72-hours.

Q5. Do you agree with the Authority's planned approach to enforcement contained in Section 5 of the Draft Procedural Guidance? If not, please explain why and propose any alternatives.

Sure does not have any specific comments about the JCRA's planned approach to enforcement. However, we wish to draw the JCRA's attention to our comments in response to Q3 where we propose that the JCRA takes a graduated approach to enforcement action.

Q6. Do you agree with the Authority's planned approach to information sharing contained in Section 6 of the Draft Procedural Guidance? If not, please explain why and propose any alternatives.

Sure does not object to the JCRA's proposed approach to information sharing and recognises that the power to share information obtained through statutory information requests and incident reporting. Indeed, we agree that there are some benefits of the JCRA being able to share such information with third parties. However, we do have questions and concerns about the extent to which this information, which will likely include information about Providers' networks and services (including potential vulnerabilities) and the existence of historic or ongoing security compromises, will be securely reviewed and stored by these third parties.

As per our query in response to Q3, we note that the JCRA is taking steps to 'securely receive, process and store confidential information'. We welcome this, but understand that no such commitment or guarantee has been made by those third parties cited in the Draft Procedural Guidance and which may be in receipt of sensitive information about Providers' security. For example, should the JCRA share sensitive information about the security of JT's network or details about a cyber incident suffered by Sure has, with the Minister or an overseas regulator, what confidence can these Providers have that the information will be handled sensitively and securely? Sure contends that this risk is particularly acute for information sharing with overseas regulators, who do not necessarily have a legitimate reason to know and understand the details of cyber incidents and security issues experienced by Providers in Jersey, and which may not have adequate facilities through which to securely receive, process, and store the sensitive information being provided.

Ultimately, Sure is concerned that, by disseminating sensitive information about the topology or security vulnerabilities of Providers' network (both of which would be available from Information Request Notice responses or incident reports) to third parties with inadequate facilities, the JCRA could actively undermine the steps it is taking to securely receive, process, and store this sensitive information. Should this information be obtained by threat actors, whether through onward compromise of the third parties' network or by inappropriate sharing by the third party, this could substantially increase the risk that these known vulnerabilities could be exploited by threat actors.

To resolve this concern, we submit that the JCRA should first seek security assurances from recipient third parties which demonstrate that the information shared shall be viewed and stored in conditions which are equivalently secure when receiving, processing, and storing information about the security of Providers in Jersey. Where the JCRA opts to ex ante or ex post notify the relevant Provider(s) that information is being shared, we request that the JCRA additionally share confirmation that the recipient third party has demonstrated that it has adequately secure facilities in which to receive, process, and store the information being shared. Alternatively, or in the event that the JCRA is unable to receive the relevant assurances, we request that the information shared with the relevant third parties be done so on an anonymised basis (i.e. there is no reference to the specific Provider in question).

In the event that a relevant third party suffers a security compromise which could place the above-mentioned sensitive information at risk, then we request that the JCRA and/or the relevant third party notify the affected Provider(s) as a matter of urgency.

Q7. Do you have any other comments on the Authority's Draft Procedural Guidance?

We note that the JCRA has distinguished the concept of "bespoke services" from those which are "publicly available in its Guidance[11]. We are grateful to the JCRA for explaining the distinction, however we believe that some more practical explanation and examples are required to enable Providers to understand what would be included within the term "bespoke services".

Can the JCRA provide clarity regarding what would be included in this definition? It is not well defined within the Guidance, nor in Ofcom's Network and Resilience Guidance/Explanatory Memorandum, and we would welcome clarification as to what types of service and/or networks are included within this definition. For example, would the following be considered as publicly

[11] Draft Telecoms Security Procedural Guidance General statement of policy under Article 24Y of the Telecommunications (Jersey) Law 2002 – page 4, paragraph 2.4.

available services or would they be considered out of scope of the Telecoms Security Framework because they are bespoke, private services:

- leased line or VPN services where the design and access are restricted to specific customers;
- secure managed service connecting a small number of premises; or
- Private mobile networks, such as private 5G networks?

Q8. Do you support the Authority's planned position on key concepts, drivers and relevant risks contained in Section 3 of the Draft Resilience Guidance? If not, please explain why and propose any alternatives.

Sure broadly agrees with and supports the JCRA's position on key concepts, drivers, and relevant risks contained within Section 3.

However, there is one aspect of Section 3 which Sure does not fully agree with or support. Sure has carefully considered Section 3 and has interpreted the section, titled "Architecture/design vulnerabilities and failings", as denoting that *all* instances of single points of failure and/or shared fate scenarios are either poor design or poor architecture. In our view, this language is somewhat absolute and fails to appropriately acknowledge nuanced scenarios where single points of failure or shared fate are unavoidable for either technical or commercial reasons. Where this is the case, we do not believe it is appropriate to describe these scenarios as simply "poor design" or "poor architecture", but rather design and architecture that takes into account technical and commercial realities (factors that are essential to a Provider). Such scenarios are, in our view, better described as proportionate design and architecture.

We believe that the key concepts and relevant risks highlighted in paragraphs 3.26 to 3.29 should be amended to recognise that, in many scenarios, single points of failure and shared fate situations are unavoidable, and therefore the presence of these design/architecture features does not necessarily indicate that a network has been 'designed poorly'.

Q9. Do you support the Authority's planned technical guidance on reliability and resilience contained in Sections 4, 5 and 6 of the Draft Resilience Guidance? If not, please explain why and propose any alternatives.

Sure does not object to any aspect of the reliability and resilience guidance outlined in Sections 4 – 6. However, Sure does have a number of queries, and requests for clarification or further information about these sections. We request that the JCRA make amendments to the finalised Resilience Guidance in accordance with the below.

Third party facilities

We note that the Resilience Guidance states in paragraph 4.3 that "[e]*ach Provider, whether at the wholesale or retail level, remains responsible for taking appropriate and proportionate measures in respect of the resilience of the network and services they are providing*"[12]. As clarified in paragraphs 4.11 to 4.13, this obligation is retained even where a Provider is reliant on a third party for part or all of that network or service[13].

We broadly support this scope and principle, however, given the extent to which third party involvement is crucial to compliance with the Law, Code of Practice, and Guidance, we would like the JCRA to expand its guidance to clarify certain specific scenarios where third party cooperation or input is required for a Provider to be able to discharge its security duties. We request that, where appropriate, the JCRA expand its Guidance (Resilience and/or Procedural) to explain its expectations

Firstly, we note from paragraph 4.13 that the JCRA expects Providers to use "contractual arrangements" to meet resilience compliance obligations. This aligns with the approach advised by the Code of Practice, which obliges Providers to, where appropriate, include certain provisions within its contracts with third party suppliers[14]. Sure does not object to either the JCRA's Guidance or the requirements of the Code of Practice. However, Sure is concerned that its relatively small size and scale could make it difficult to obligate third party suppliers, some of which have global size and scale, to amend contracts or provide information. In our view, this is likely to be a concern for many Providers in Jersey.

As the JCRA are aware, the telecommunications industry is technically complex and heavily influenced by economies of scale and scope. The consequence is that Sure, and other Providers in Jersey, often need to engage with third party suppliers which are significantly larger in terms of scale, size, and resources. This means that Sure's buyer power when engaging with these large multinational organisations is somewhat limited. ✂

We would welcome guidance from the JCRA for scenarios in which the supplier, partner, or peer refuses to agree to certain SLAs or contractual provisions, or refuses to provide information that enables the Provider to suitably consider and manage risks. Specifically, should such a scenario occur, what approach would the JCRA expect Providers to take to either (a) address the risk via another route, or (b) take further action to ensure such SLAs, contractual provisions, or other processes are put in place.

[12] Draft Telecoms Security Resilience Guidance – page 17, para. 4.3.
[13] Draft Telecoms Security Resilience Guidance – page 19, para. 4.11 – 4.13.
[14] See, for example, Third Party Supplier Measures 3, located on pages 95 – 103.

We understand that Ofcom has advised UK Providers to notify it and the NCSC where UK Providers receive pushback or rejection from major suppliers, but we are not aware of what action Ofcom and/or the NCSC would seek to take.

Secondly, the Draft Resilience Guidance makes reference to the use of shared facilities[15]. This is another topic for which Sure would appreciate further guidance because it makes use of shared facilities in Jersey to facilitate its network and provide services. Can the JCRA please clarify or expound on its expectations for the following issues?

- Where Providers must undertake risk assessments for shared facilities (such as assessing natural phenomena risks or human risks), does the JCRA expect the Provider to undertake a complete assessment for those shared facilities even where the Provider does not own/operate the facility? Examples of this for Sure include data centres in which Sure locates its active equipment but does not own the data centre facility. Alternatively, Sure utilises shared office space in a building for which it is not the owner. In these examples, Sure is unable to undertake a comprehensive risk assessment because it does not have access to all relevant information. In these circumstances, can Sure (or another Provider) discharge its obligations by requesting that the facility owner/operator undertake the risk assessment on its behalf?

- For shared facilities where a permanent electricity generator is required, can the JCRA please clarify what a Provider must do should a host location refuse permit the use of a generator which can be refilled? We are concerned that, due to the significant cost and disruption of needing to move a core network or core network elements, it is unlikely to be proportionate or appropriate to move the site on the basis that a host refuses to permit the use of generators. In such circumstances, how would the JCRA expect Providers to best discharge their security obligations? Given the need for seamless automatic failover at larger aggregation and core network sites, would it be acceptable for such a site not to have permanent electricity generators provided that, should loss of power occur at the site, failover occurs to another site with generator backup?

Finally, the Draft Resilience Guidance refers to "regularly review" of security matters with suppliers, partners, and peers. Can the JCRA give further guidance on this topic? On the assumption that a risk-based approach is taken by a Provider, what would be sufficient regularity for a review with a high risk supplier compared against a lower risk supplier? Should the supplier be higher risk, would one review per contractual cycle be sufficient in the eyes of

[15] Draft Telecoms Security Resilience Guidance – page 15, para. 3.26.

the JCRA or would annual reviews be required? Understanding the JCRA's expectations on this topic will enable Providers to plan and implement reviews which align with JCRA expectations.

'Remote distribution facilities'

In paragraphs 4.29 and 5.23 (including the header to the latter section), the JCRA uses the term "remote distribution facilities". Whilst we understand that these facilities will form part of a Provider's aggregation network, we are not familiar with the term and would welcome an explanation and examples of what the JCRA considers to be a "remove distribution facility".

Can the JCRA please clarify what it means by "remote distribution facilities" in the context of a fixed network? Where possible, can some examples be included in the Resilience Guidance?

User-hours lost

We welcome the JCRA's description and explanation of "user-hours lost"[16] and support the use of the concept for risk assessment, network architecture, and reporting purposes as explained in paragraphs 5.33 to 5.38 of the Draft Resilience Guidance.

Notwithstanding this broad support, we don't believe that the concept of "user-hours lost" will always be appropriate for risk assessment, design, and reporting for mobile networks and services. In Sure's experience, the mobile environment is significantly more dynamic than that of fixed networks because mobile subscribers and their devices move around the island and therefore will move between mobile sites. The corollary is that the number of subscribers attached to any one mobile radio access network ("RAN") site, and thus the number of subscribers served by, or reliant on, a given aggregation/backhaul facility, will change over time. Indeed, whether a mobile site could, in the event of failure, generate a high "user-hours lost" could depend on the time of day or the day of the week. It can therefore be difficult for a Provider to calculate the exact number of users impacted by a notional outage at a given mobile RAN site, which inhibits a Provider's ability to accurately calculate the "user-hours lost".

Sure has, to date, used the concept of "utilisation" as the key metric for determining the importance of individual mobile RAN sites. Utilisation looks at a variety of factors, such as active users (where possible), throughput, baseband load, scheduler and timeslot utilisation, and power output. That is, Sure's mobile engineering team considers a variety of factors when determining whether a given mobile RAN site is significant for its network and end-users.

We therefore request that the JCRA permit the use of other utilisation factors, such as the above-mentioned, when making architectural, design, operational, and reporting decisions within the context of the Resilience and Procedural Guidance. Should it be happy for Providers

[16] Draft Telecoms Security Resilience Guidance – page 30, Box 1.

to do so, can the JCRA explicitly confirm this in its finalised Resilience and Procedural Guidance?

Spare equipment stores

Paragraph 6.14 and 6.15 of the Draft Resilience Guidance explains that Providers should put in place "appropriate support arrangements", including 'pre-emptively building up spare equipment stores of hardware stock'[17].

We broadly support the Draft Resilience Guidance's position that supplier management is critical and that Providers of networks and services should pre-emptively build up a stock of spare hardware components. We therefore agree with the Draft Resilience Guidance as drafted. However, our experience and engagement with the JCRA on the topic of T-049 Telecoms service incidents (May-July 2023)[18] ("the T-049 Case") and the JCRA's comments made in Annex C to the Final Decision, dated 11th November 2024[19], means that we believe the topic of spare hardware components should be considered further in the context of the Resilience Guidance. We submit that further guidance on this topic should be provided by the JCRA within the finalised Resilience Guidance.

In the first instance, we do not believe there is sufficient guidance on the topic of spare hardware components within the Draft Resilience Guidance. Given that there are many approaches to dimensioning a Provider's spares inventory, and that the JCRA may have a preference as to the way in which spare hardware components are retained, it is not sufficient to simply state that Providers should "pre-emptively build up dedicated spare equipment stores". For example, does the JCRA expect Providers to take a risk-based approach when deciding which spares to hold or should Providers hold spares for all network components? Similarly, would the JCRA expect spares to be held locally or within any of the British Islands (as per the Code of Practice)? We contend that the Resilience Guidance would be more helpful if the JCRA made its expectations explicit, particularly given it is the JCRA and Government of Jersey which are setting the service level targets and regulatory obligations.

Furthermore, we believe that the Resilience Guidance represents an opportunity for industry to discuss Providers' approach to holding spare hardware components and agree a best-practice approach. We submit that such a discussion is required because, in our view and based on our experience in the T-049 Case, the JCRA's position on holding spares does not necessarily align with Sure's approach (and likely the approach taken by other Providers).

[17] Draft Telecoms Security Resilience Guidance – page 49, para. 6.15.
[18] Final Decision on Licence Contraventions and Reasonable Steps Case T-049: Telecoms service incidents (May-July 2023)
[19] Final Decision Annex C: Authority Response to Sure's Response of 6th September

During the T-049 Case, the JCRA indicated that it expected Sure to have held spares for *all* system components. ✂ Were Providers to be obliged to hold spares for all, or the majority of, its hardware components, this would entail holding thousands, or tens of thousands, of spare network components. The corollary would be that Providers would tie up very substantial amounts of cash in stock that may ultimately go unused (money will be spent on spare components that don't get used, become end of life or out of date, then get written down) placing the wider business under unnecessary financial pressure. We submit that this would be disproportionate given real and relevant commercial pressures faced by Providers of telecommunications networks and services.

Conversely, we submit that a risk-based approach to dimensioning a Provider's spare hardware component stock list is both appropriate and proportionate. It allows Providers to appropriately address the risk of network failure whilst also responsibly managing the organisation's financial resources. Whilst a risk-based approach can result in occasions where the requisite network component is not immediately available, we contend that such an outcome would be rare and still preferable to a scenario in which Providers are placed in financial difficulty (or financially wasteful at a minimum) by onerous regulatory obligations.

✂ we would appreciate some guidance and clarification from the JCRA, which should be set out explicitly in the Resilience Guidance. Specifically, we would like the JCRA to explain:

- What approach it expects Providers to take when building its store of hardware spares (a risk-based approach or an alternative)?
- If an alternative approach, what does this entail and why is it appropriate and proportionate?

For the avoidance of doubt, Sure submits that the most appropriate and proportionate approach to spare stock management is for Providers to take a risk-based approach.

Testing

The Draft Resilience Guidance explains that testing and validation should occur before changes to existing services occur[20]. The Draft Resilience Guidance then goes on to briefly explain the nature of the testing expected by the JCRA.

Whilst we broadly agree with the Draft Resilience Guidance on this topic, we note that the Guidance does not appear to make provision for emergency planned works. That is, for changes

[20] Draft Telecoms Security Resilience Guidance – page 51, para. 6.25.

to existing networks and services that need to be implemented quickly due to emergency conditions. In Sure's experience, it is not always possible to undertake testing and/or validation where a network or service change needs to be made at short notice. This is particularly the case where a change needs to be made as soon as possible in order to preserve or restore services to end-users.

Consequently, we request that the JCRA consider additional and differing guidance for planned emergency network and/or service changes.

Q10: Do you have any other comments on the Authority's Draft Resilience Guidance?

We note that these Draft Resilience Guidelines asserts that it supersedes and replaces certain JCRA Guidelines which are currently in force. At paragraph 2.32 of the Draft Resilience Guidance, the JCRA states that the Resilience Guidance shall 'supersede and replace any previous guidance given by the JCRA on general network and service resilience and reliability'[21].

Can the JCRA please confirm the extent to which the Resilience Guidance, and also the Procedural Guidance, supersedes and replaces the 999 Guidance[22]? Sure's interpretation of paragraph 2.32 is that the 999 Guidance is superseded and replaced by the new Resilience and Procedural Guidance, but would welcome clarification. If the JCRA is of the view that the 999 Guidance is superseded and replaced, could the JCRA confirm whether this is the entirety of the 999 Guidance or simply parts of the 999 Guidance? For example:

- when reporting service incidents to the JCRA, should Providers use the metrics outlined in paragraph 3.26 of the 999 Guidance, or in Table 1 and Table 2 of the Procedural Guidance?
- Will notifications about a service incident involving 999 be done using a secure communication method and information requirements documented in paragraphs 4.38 to 4.66 of the Procedural Guidance, or the information requirements documented in 3.29 of the 999 Guidance?
- Will aspects of the 999 Guidance which do not feature in the Procedural Guidance or Resilience Guidance, such as the VoIP Considerations, be retained? If so, in which document will this information be retained?

[21] Draft Telecoms Security Resilience Guidance – page 8, para. 2.32.
[22] t-116-update-999-guidance-final-guidance.pdf

Should the JCRA confirm that the 999 Guidance will be replaced by the Resilience and Procedural Guidance, then we request that the 999 Guidance be formally withdrawn so as to avoid confusion between conflicting documents.