STATES OF JERSEY

DRAFT TELECOMMUNICATIONS LAW (JERSEY) AMENDMENT REGULATIONS 202- (P.47/2024) – COMMENTS

Presented to the States on 27th August 2024
by the Economic and International Affairs Scrutiny Panel

STATES GREFFE

COMMENTS

Introduction

1. The Draft Telecommunications Law (Jersey) Amendment Regulations 202- ('the Regulations'), lodged by the Minister for Sustainable Economic Development ('the Minister'), aim to address the pressing need for enhanced security and resilience in Jersey's telecommunications infrastructure. These networks are essential to Jersey's critical national infrastructure, underpinning both the economy and the daily lives of its residents. In the face of escalating global cyber threats, this legislation seeks to protect Jersey's communications networks from risks posed by both nation-states and organised crime.

2. The Economic and International Affairs Panel ('the Panel') welcomes the effort to align Jersey's regulatory framework with international best practices, particularly the United Kingdom's (UK) Telecommunications (Security) Act 2021, while recognising the need to adapt certain provisions to Jersey's unique context. Given the critical role of telecommunications in Jersey's status as an international financial centre, ensuring robust security for both businesses and residents is of paramount importance.

Legislation Background

3. Telecommunications networks are an integral part of Jersey's national infrastructure, supporting economic activities and essential services. The Panel understands that the security of these systems is increasingly critical, given the threat of cyber-attacks from sophisticated nation-state actors such as Russia, China, and North Korea, as well as organised crime groups and other bad actors. The National Cyber Security Centre (NCSC) has highlighted the significant risks posed by such threats, reinforcing the necessity for a comprehensive and resilient security framework.

4. The Regulations build on the UK's Telecommunications (Security) Act 2021, itself influenced by European telecoms legislation, specifically the European Electronic Communications Code 2018 Directive (EU) 2018/1972. Given Jersey's use of the UK +44 area code and close economic and regulatory ties with the UK, aligning with UK legislation is critical to ensure consistency with international best practices. However, it is equally important that the Regulations are carefully tailored to reflect Jersey's smaller market and specific needs, ensuring they remain proportionate and effective.

5. The Regulations introduce new security obligations for Jersey's public communications providers, mandating proactive measures to prevent, identify, and address security threats to their networks. The Panel notes that the Jersey Competition Regulatory Authority (JCRA) will have an expanded role in enforcing these requirements, ensuring that public communications providers meet their security responsibilities.

Scrutiny Work to Date

6. The Panel has undertaken extensive scrutiny of the Telecoms Security Framework workstream, including consultations with key stakeholders and the Government, to assess the implications of the legislation.

7. As part of its review of the Government Plan 2023-2026, the Panel noted that £242,000 had been allocated for specialist expertise to develop a telecoms security framework aligned with the UK's 2021 Telecommunications Security Act. The Panel emphasised the importance of this funding in ensuring the security of Jersey's telecommunications infrastructure, especially given the critical nature of the +44 area code and the need for alignment with UK regulations.

8. In a letter dated 4th October 2023, the Panel was informed that progress had been made in collaboration with telecoms companies, the JCRA, and the Law Drafting Office. However, the lodging of the Regulations had been delayed to incorporate feedback from stakeholders, ensuring that the framework would be proportionate and effective for Jersey's unique telecommunications landscape.

9. During a public hearing on 11th April 2024 public hearing, the Panel discussed the Regulations with the Minister and Officers. It was confirmed that the new framework would enable the Government of Jersey ('the Government') to issue orders to telecoms providers, including mandates for the removal of high-risk equipment. The Panel was reassured that Jersey's telecoms security framework would broadly mirror the UK's legislation, tailored to the Island's needs.

10. As part of its ongoing scrutiny of the workstream, the Panel received private briefings from Government Officers on 7th March 2024 and met with the JCRA on 4th April 2024.

Panel Observations

Dual Role of the JCRA

11. The Panel notes the JCRA's dual function as both the telecoms security regulator and competition authority. This differs from the UK model, where Ofcom regulates telecoms and the Competition and Markets Authority (CMA) oversees competition. The Panel questioned whether this consolidation of authority could lead to conflicts of interest, particularly when smaller providers may struggle to comply with new security measures.

12. During the public hearing on 11th April 2024, the Minister explained that the dual role was necessary given Jersey's smaller market and that separating the two functions would not be cost-effective. The Panel accepts that additional considerations must be made, but would highlight that the JCRA, in balancing competition and security, may face challenges in addressing the needs of smaller operators disproportionately affected by stringent security requirements.

13. The Regulations provide the JCRA with extensive enforcement powers, including the ability to gather information, conduct inspections, and issue

compliance notices. These powers are designed to ensure that telecom providers adhere to security standards, while maintaining Jersey's alignment with international best practices through collaboration with the NCSC and other regulatory bodies.

Impact on Competition

14. The Panel's concerns regarding competition are particularly relevant, especially noting the merger between Airtel-Vodafone and Sure. This merger will result in the reduction of the number of mobile network operators in the Channel Islands from three to two—namely JT and Sure. The JCRA initially expressed concerns that this reduction in providers would lead to a "substantial lessening of competition". Airtel, despite being the smallest of the three providers, held a significant market share (25%), and its presence helped aid in competitive pricing and service options.

15. The merger has now been conditionally approved, but the JCRA attached several conditions to mitigate the impact on competition. These include the introduction of a new competitor, the Channel Islands Co-op, which will operate as a Mobile Virtual Network Operator (MVNO) using Sure's infrastructure. This addition is expected to ensure that consumer choice remains available and competitive.

16. Furthermore, the JCRA imposed pricing commitments that protect current consumer prices for 36 months post-merger. This safeguard aims to prevent any immediate price hikes due to the reduced number of competitors, giving time for the Co-op's entry to stabilise the market.

17. Concerns about the merger highlight the importance of ongoing consultation with stakeholders to ensure that the interests of consumers and smaller market players are protected. The involvement of the Co-op's new mobile network, which promises to increase consumer choice while relying on Sure's infrastructure, would appear to be a key component of the JCRA's strategy to mitigate potential negative impact. The Panel will closely monitor the market as these changes unfold, ensuring that competition remains healthy and consumers continue to benefit from a variety of service providers.

Cybersecurity and Resilience

18. In addition to its focus on competition, the Regulations place significant emphasis on improving cybersecurity and resilience within Jersey's telecoms infrastructure, this is particularly pertinent given the increasing global threats from cyber-attacks. The Panel understands that Jersey's ability to defend its critical national infrastructure from such threats is vital to the Island's economy, particularly the finance sector, which relies heavily on secure and resilient telecoms networks.

19. The proposed merger between Sure and Airtel-Vodafone is also framed within the context of improving resilience. Sure has committed to investing £48 million in a new 5G network across the Channel Islands, which is expected to bring faster data speeds, wider coverage, and a more secure mobile network. Sure's commitment to adhering to High-Risk Vendor (HRV) regulations ahead

of schedule underscores the importance placed on cybersecurity in the merged network.

20. The Regulations propose that telecom providers in Jersey will be tasked with identifying vulnerabilities and upgrading their systems to mitigate these risks. The draft regulations reinforce this by placing new duties on public communications providers to take proactive measures to secure their networks.

21. This includes specific security requirements related to network architecture and vendor procurement, ensuring that telecoms providers are not using equipment or services from high-risk vendors. The role of the JCRA in overseeing compliance with these security measures is critical, as they will have the power to issue notices and gather information from providers on the security of their networks

22. The combination of regulatory oversight and industry investment is expected to enhance Jersey's resilience against cyber threats. However, the Panel recognises the importance of continuous scrutiny to ensure that these investments lead to tangible improvements in security and do not inadvertently place smaller operators at a disadvantage.

23. The Panel notes that the Regulations provide both the Minister and the JCRA with the ability to impose penalties should providers contravene their legal duties. Those penalties have been set to a maximum of 10% of turnover of the provider's business, or £10,000 per day for continuing offences.

Further Considerations

24. The guidance from the NCSC stresses the necessity of clear, actionable implementation guidelines. The NCSC's Telecoms Security Requirements (TSRs) provide a structured approach to reducing cyber risks by implementing practical security controls. In Jersey, the Minister and the JCRA will be expected to issue these guidelines, ensuring compliance among telecoms providers and maintaining a secure environment for Jersey's communication networks.

25. Engagement with telecom providers will be crucial in developing guidelines that are feasible yet effective and should be based on collaboration between the public and private sectors, ensuring that telecoms providers can comply without undue operational burdens. This aligns with the International Security Alliance (ISA) recommendations, which advocate for a deeper public-private partnership to balance the needs of businesses, governments, and customers.

International Developments

26. A significant component of both the NCSC and the Regulations is the management of HRVs. The Government of Jersey will follow UK precedent, where high-risk vendors have been gradually phased out of critical network infrastructures to avoid national security risks.

27. This phasing out aligns with the work of United States of America's Federal Communications Commission's (FCC) actions to bar specific providers from

certifying wireless equipment due to national security concerns offer another comparison, highlighting how international regulations and actions shape national telecom security frameworks. Jersey's guidelines should reflect this international trend, ensuring security and trust in its telecom infrastructure.

28. Internationally, telecoms security has become increasingly politicised, particularly concerning supply chain risks from high-risk vendors. The ISA underscores the need for countries to develop multi-dimensional cybersecurity frameworks that address the complex threats posed to telecom networks. Jersey can draw from the FCC (United States of America) and NCSC (UK) policies, which seek to mitigate risks by diversifying supply chains and imposing restrictions on vendors who are high risk.

29. The Panel notes Jersey's prominent role in the Small Nations Regulatory Forum, which could play a vital role in helping align its telecoms security with global best practices by learning from similarly sized jurisdictions. The forum would allow knowledge sharing between smaller jurisdictions facing similar risks from high-risk vendors and global cyber threats. Jersey can benefit from shared resources and collaborative testing, similar to the UK's National Telecoms Lab, which provides a research environment for testing network security.

30. The Panel would highlight that elements within the UK's 5G Diversification Strategy, for instance, include a model that includes not only banning high-risk vendors but also investing in alternatives like Open Radio Access Network (Open RAN) technology. Jersey could similarly explore investment in diversified telecom technologies, reducing reliance on a few dominant suppliers and encouraging innovation within its own telecommunications infrastructure.

Challenges and Recommendations

31. One of the core challenges outlined in the ISA report is ensuring trust between governments, telecom providers, and customers. This is particularly crucial in data privacy and incident reporting, where the interests of customers, businesses, and governments may seem at odds. However, transparent regulations and clear communication protocols can help reconcile these interests, ensuring that data access is lawful and auditable, as recommended by both the NCSC and ISA.

32. The Panel notes that both the NCSC and ISA reports highlight the need for efficient incident reporting to mitigate telecom risks. Jersey's public-private partnerships should emphasise the importance of swift, transparent communication during security breaches, with the Government's guidance ensuring that responses remain proportionate and effective.

33. The Panel also recognises the important role of the Jersey Cyber Security Centre (JCSC) in supporting the Island's cyber resilience. Established in 2021, the JCSC offers free and confidential advice on cyber security and works closely with relevant authorities when needed. Its involvement in an international cyber emergency response network ensures that Jersey stays informed on the latest threats and best practices. With work ongoing to develop the draft Cyber Security Law, the JCSC's role in enhancing telecoms security will be further

strengthened, making it a key player in safeguarding Jersey's telecoms infrastructure.

34. Another key point from the ISA report is the challenge posed by rapid technological changes as traditional regulations may lag behind global innovation, impeding service delivery or stifling investment. This concern is mirrored in the NCSC's emphasis on flexibility, where security frameworks must evolve alongside emerging threats and technologies.

35. The Panel stresses Jersey's telecom regulations must remain adaptable to technological changes. Investment in future-proof networks, such as virtualised cloud-based systems, can help the telecom sector keep pace with advancements in cyber threats while maintaining security.

Conclusion

36. To conclude, the Panel is broadly in agreement with the proposed Regulations, whist noting their practical implementation will be undertaken following further the issuance of guidance by the Minister and JCRA. The Panel believes that sufficient consultation and engagement with stakeholders within the industry will be critical to the successful safeguarding of the Island's telecoms infrastructure without unduly burdening providers or hindering markets.

37. In considering the Regulations, the Panel encourages the States Assembly to remain aware of the guidance from the NCSC, ISA, and other international examples. The combination of robust implementation guidelines, stakeholder management, and alignment with international standards will be crucial to securing its telecommunications infrastructure.

38. Key considerations include:

    a. Managing high-risk vendors through gradual phasing out and the development of diversified supply chains, similar to the UK's and US's approach.

    b. Encouraging innovation in telecoms security by investing in Open RAN and virtualised infrastructure, which can bolster both security and operational flexibility.

    c. Fostering collaboration within the Small Nations Regulatory Forum to ensure Jersey's telecoms network remains aligned with global best practices, sharing resources and strategies with other small jurisdictions.

39. Finally, the Panel believes that Government should continue to focus on maintaining trust, adaptable regulation, and international collaboration to secure its telecommunications infrastructure in the face of evolving threats.