T-062 Telecoms Security

Consultation on Draft Procedural Guidance (Statement of Policy) and Resilience Guidance

Document No: JCRA 25/19

Publication date: 8 August 2025

Closing date: 17 October 2025

Jersey Competition Regulatory Authority
2nd Floor Salisbury House, 1-9 Union Street, St Helier, Jersey, JE2 3RF
Tel 01534 514990

Web: www.jcra.je

Contents

1 Overview and summary

Through amendments made to Jersey's telecommunications law in September 2024, the Jersey Competition Regulatory Authority (the **Authority**) receives new legal powers and duties under a telecoms security framework being introduced by the Government of Jersey.

Among the new duties is a requirement for the Authority to prepare and issue a statement of its general policy with respect to the exercise of its telecoms security functions under the local telecoms law. This general policy is contained in the Draft Procedural Guidance document appended to this document as Annex 1.

Before issuing this Procedural Guidance, the Authority must bring it to the attention of those who will be affected by it. The purpose of this consultation is to ensure telecoms providers have an opportunity to review and comment on a draft version of the proposed Procedural Guidance before the Authority issues a final version.

The amended law imposes a legal duty for telecoms providers to identify, reduce and prepare for compromises to the availability, performance or functionality of their networks or services. To help telecoms providers understand the expectations associated with the requirement, the Authority has created Draft Resilience Guidance, which is appended to this document as Annex 2. This consultation also ensures that telecoms providers have an opportunity to review and comment on this Draft Resilience Guidance before the Authority issues a final version.

In connection with these two draft guidance documents, the Authority welcomes responses to the following questions:

Question 1: 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?

Question 2: Do you have any comments on the Authority's approach to developing its Draft Procedural Guidance and Draft Resilience Guidance?

Question 3: 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.

Question 4: 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.

Question 5: 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.

Question 6: 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.

Question 7: Do you have any other comments on the Authority's Draft Procedural Guidance?

Question 8: 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.

Question 9: 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.

Question 10: Do you have any other comments on the Authority's Draft Resilience Guidance?

This consultation closes on 17 October 2025. After assessing responses received, the Authority plans to issue final versions of the Procedural Guidance and Resilience Guidance prior to assuming its functions under the amended telecoms law. Section 4 of this document explains how to respond to the consultation.

2 Introduction and background

2.1 This section introduces the consultation and provides background information on the Draft Procedural Guidance and Draft Resilience Guidance. Its contents include:

- Purpose of document
- Jersey's new telecoms security framework
- The Government's consultation on its Draft Security Measures Order and Draft Code of Practice
- Legal and regulatory context
- The planned process and timetable

Purpose of document

2.2 This document is a consultation on the Authority's proposed guidance to Providers in connection with its powers and duties relating to Jersey's telecoms security framework. These documents are:

- **Draft Procedural Guidance** explaining the processes operated by the Authority to deliver its telecoms security functions.
- **Draft Resilience Guidance** explaining expectations associated with designing and operating inherently reliable networks and services.

2.3 The purpose of this consultation is to bring these two draft guidance documents to the attention of providers of public electronic communications networks and services (**Providers**) with legal obligations to design and operate secure and resilient networks and services.

Jersey's new telecoms security framework

The need for a new framework

2.4 In September 2024, the States Assembly passed the Telecommunications Law (Jersey) Amending Regulations 2024 (the **Amending Regulations**), which amended the Telecommunications (Jersey) Law 2002 (the **Law**)[1] with the aim of increasing the security of Jersey's vital telecoms sector through creating a new telecoms security framework.[2]

2.5 In a consultation introducing the Amending Regulations, the Government of Jersey (the **Government**) explained factors leading to new legislation for securing the Island's communications networks and services which include protecting the Island's economy, positioning Jersey as a centre for innovation and ensuring Islanders have reliable, secure digital connectivity to the world.[3]

[1] States of Jersey: Telecommunications (Jersey) Law 2002 as amended on 1 October 2024 – see here for more information.
[2] States of Jersey: Draft Telecommunications Law (Jersey) Amendment Regulations 202- (P.47/2024) – Comments – see here for more information.
[3] Government of Jersey: Consultation: Telecoms Security Framework (July 2023) – see here for more information.

2.6 Within the 2024 consultation, the Government also stated its intention to base its approach to amending the Law on UK legislation which came into force in 2021, underlying the importance of Jersey's relationship with the UK and the close and beneficial relationship between local Providers and their UK counterparts based on shared use of the +44 number range.

About the telecoms security framework

2.7 Aligned with the UK approach, Jersey's new telecoms security framework consists of several closely interrelated components:

(a) Underpinning legislation establishing expectations and responsibilities focused on two key aspects of telecoms security:

i. A range of security measures for adoption by Providers to enhance protection against cyber and resilience incidents; and

ii. A requirement to remove equipment supplied by companies considered a risk to Jersey's security.

(b) A list of defined security measures that Providers must implement (the **Security Measures Order**).

(c) Guidance on how Providers can demonstrate compliance with implementing the Security Measures Order (the **Code of Practice**).

2.8 While the framework applies to all Jersey Providers, the Security Measures Order and Code of Practice only apply to those named in the Security Measures Order, although all Providers could choose to adopt any aspects of the measures and guidance they consider appropriate for their networks and services.

2.9 Under the framework, the Authority also receives new powers and duties, which include issuing guidance on its operational approach for monitoring and managing compliance and explaining expectations for operating reliable and resilient networks and services.

The Authority's role in the framework

2.10 Under Article 24V of the Law, the Authority has a general duty to seek to ensure that Providers comply with their security duties under the new telecoms security framework and take steps to address any contraventions where the Authority has reasonable grounds to do so. This remit encompasses working with Providers to monitor and improve the security of their networks and services.

2.11 The framework also provides the Authority with certain security functions including receiving reports from Providers on the risk and occurrence of security compromises and reporting and sharing information with others in the interests of the security of Jersey or in connection with the prevention, detection or investigation of crime.

2.12 The Law requires the Authority to issue a Statement of Policy (the Procedural Guidance) explaining how it intends carrying out its security functions, for the purpose of establishing principles and setting

expectations for Providers with duties under the Law and who are obliged to demonstrate compliance. This consultation seeks views on the Authority's Draft Procedural Guidance (see Section 3 for more information).

2.13 Under the Law, the definition of a security compromise includes both "cyber security type" compromises such as those caused by malicious actors, and resilience related compromises reflecting a broad range of other factors that impact on the availability of public communications networks and services. These include impacts caused by external factors, such as floods, cable cuts or power cuts, or internal factors, such as hardware failures, operational process errors or network design flaws. This consultation further seeks views on the Authority's Draft Resilience Guidance relating to the reliability and resilience of networks and services (see Section 3 for more information).

The Government's consultation on its Draft Security Measures Order and Draft Code of Practice

2.14 Although the States Assembly passed the Amending Regulations in September 2024, certain elements of the telecoms security framework – specifically those relating to security measures and the Code of Practice – were not enacted at that time.

2.15 In July 2025, the Government began the process of enacting the elements of the Law relating to security measures and associated guidance by issuing a consultation on the proposed Security Measures Order and Code of Practice.[4] Subject to the outcome of this consultation, the States Assembly will be asked to consider and adopt the Security Measures Order and agree to issue the Code of Practice.

2.16 Mindful that the adoption of the Security Measures Order and issuing the Code of Practice will bring into effect its telecoms security framework powers and duties under the Law, the Authority has prepared and is consulting on its proposed security function and guidance to Providers.

Legal and regulatory context

2.17 Article 7(1) of the Law places an overarching duty on the Authority to ensure that telecoms services exist in the Island and between Jersey and the rest of the world to meet all current and future demand and Article 7(2)(c) requires that it performs its duties in a way that will best further the economic interests of Jersey.[5]

2.18 In its introduction to the Amending Regulations, the Minister for Sustainable Economic Development highlighted the need to protect Jersey's economy, and the daily lives of Islanders, through addressing the pressing need for enhanced security and resilience in Jersey's telecoms infrastructure, noting that communications networks are essential to Jersey's critical national infrastructure.[6]

[4] Government of Jersey: Consultation: Proposed Jersey Telecoms Security Order and Code of Practice – see here for more information.
[5] States Assembly: Telecommunications (Jersey) Law 2002, Article 7(2)(c) – see here for more information.
[6] States Assembly: Draft Telecommunications Law (Jersey) Amendment Regulations 202- (P.47/2024) – Comments – see here for more information.

2.19 The Amending Regulations created Part 5A of the Law introducing new security obligations on Jersey's Providers, requiring them to take measures to prevent, identify and address security threats to their networks and services and provide an expanded role for the Authority to enforce these requirements, ensuring that Providers meet their security responsibilities.

2.20 Article 24Y of the Law requires the Authority to prepare and publish a statement of its general policy about its security functions under the Law and must ensure it is brought to the attention of persons it is likely to affect. This consultation on the Authority's Draft Procedural Guidance fulfils this requirement.

2.21 Under Article 7(3)(c) of the Law, the Authority shall have regard to whether telecoms services are of high quality and reliable, which it interprets as a positive duty to ensure the networks and services of Providers are inherently reliable and resilient for the benefit of Jersey's economy and the daily lives of Islanders.

2.22 Article 24K(2) defines anything that compromises the reliability and resilience of the network and/or that causes signals conveyed by means of the network or service to be lost as a security compromise. Article 24M requires Providers to take appropriate and proportionate measures to stop a security compromise causing adverse effects and if this happens, to take appropriate and proportionate measures to remedy or mitigate that effect.[7]

2.23 To support its duties under the Law and in line with best practice regulatory principles, the Authority plans to issue guidance for Providers that are required to operate reliable and resilient networks and services. This guidance will help Providers understand what measures are considered appropriate and proportionate to prevent security compromises from causing adverse effects or to remedy and mitigate those effects if they occur. This consultation on the Authority's Draft resilience Guidance fulfils this requirement.

The planned process and timetable

2.24 The timetable, which may be subject to change, for completing the process is:

Aug 2025	Issue consultation on Draft Procedural Guidance and Draft Resilience Guidance
Oct 2025	Close consultation and consider responses / information received
Q1 2026	Issue final Procedural Guidance and Resilience Guidance and assume powers and duties under the Law

Question 1: 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?

[7] Those telecoms providers who are subject to a licence from the Authority under the Law are also bound by licence conditions which impose obligations in relation to the resilience of their networks.

3 About the Draft Procedural Guidance and Draft Resilience Guidance

3.1 This section explains the purpose and summarises the contents of the Draft Procedural Guidance and Draft Resilience Guidance. Its contents include:

- Development approach
- About the Draft Procedural Guidance
- About the Draft Resilience Guidance

Development approach

3.2 As explained in Section 2 above, the Authority has a legal requirement to issue Procedural Guidance under the Law and a regulatory commitment to issue Resilience Guidance.

3.3 The Government has chosen to closely follow the UK's Electronic Communications (Security Measures) Regulations and Code of Practice[8] when developing its own equivalent regulations and guidance, after working closely with UK Government agencies to ensure this approach was proportionate and appropriate for Jersey.

3.4 Taking account of this approach, the Authority has aligned its approach to developing its Procedural Guidance and Resilience Guidance with equivalent frameworks issued by the UK communications regulator Ofcom, while considering and taking account of local context. The benefits of this are as follows:

i. It extends the Government's synergistic approach of aligning with the UK Government's approach to telecoms security, which it has strongly prioritised in developing and implementing a comprehensive telecoms security framework.

ii. It underpins and helps protect Jersey's vital connectivity arrangements with the UK, through which the Island has access to the +44 number range, extensive telephony interconnections and internet peering arrangements.

iii. It allows the Authority to efficiently draw on best practice in its approach to monitoring and managing its role in the telecoms security framework and creates opportunities to identify and assess future telecoms security development requirements.

Question 2: Do you have any comments on the Authority's approach to developing its Draft Procedural Guidance and Draft Resilience Guidance?

[8] UK Government: Electronic Communications (Security Measures) Regulations and Telecommunications Security Code of Practice – see here for more information.

About the Draft Procedural Guidance

3.5 The Procedural Guidance provides relevant information to Providers on the Authority's approach to its telecoms security functions under the Law, and explains the associated procedures that Providers should be aware of and follow.

3.6 It contains the following sections:

(a) **Compliance monitoring**: The Authority will seek to ensure that Providers comply with security duties imposed on them under the telecoms security framework, which means taking a proactive approach to monitoring and ensuring compliance. The Draft Procedural Guidance explains how the Authority plans to use its powers to gather information on how Providers are meeting or planning to meet the legal requirements contained in the Security Measures Order. This section includes information on the Authority's general policy on testing requirements.

(b) **Reporting security compromises**: Under the Law, Providers will have duties to report both the risk and occurrence of security compromises when Part 5A commences. The Draft Procedural Guidance explains the Authority's planned incident reporting processes, provides illustrative examples of reportable cyber security compromises and defines the associated thresholds and criteria for reporting.

(c) **Enforcement**: The Authority may consider enforcement action where it determines there are reasonable and appropriate grounds for doing so. The Draft Procedural Guidance explains the Authority's planned general approach to enforcement, the legal framework to follow and power to impose penalties.

(d) **Information sharing**: The telecoms security framework recognises the benefits of sharing information with others involved in telecoms security for the purpose of helping the Authority and others to perform their functions, and establishes certain statutory information sharing gateways to enable this. The Draft Procedural Guidance explains the Authority's planned approach to information sharing and establishes a framework for its practical operation.

Question 3: 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.

Question 4: 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.

Question 5: 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.

Question 6: 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.

Question 7: Do you have any other comments on the Authority's Draft Procedural Guidance?

About the Draft Resilience Guidance

3.7 The Resilience Guidance provides guidance for Providers required by the Law to design and operate inherently reliable communications networks and services or having obligations under their licences to operate a resilient and reliable network. While the information it contains is not legally binding, the Authority may take it into account in enforcement actions. Providers may choose to comply with their resilience-related security duties by adopting different technical solutions or approaches to those specified in the document.

3.8 It contains the following sections:

(a) **Key concepts, drivers and relevant risks**: The concept of resilience as it relates to Jersey communications networks and services is wide, linked to several interrelated factors and requires Providers to adopt a planned approach to identifying and managing associated risks. Section 3 of the Draft Resilience Guidance examines this and explains the Authority's considerations.

(b) **Technical guidance on reliability and resilience**: The Amending Regulations require Providers to take appropriate and proportionate measures to stop a security compromise causing adverse effects and if this happens, to take appropriate and proportionate measures to remedy or mitigate that effect. Sections 4, 5 and 6 of the Draft Resilience Guidance explains the Authority's technical guidance on how Providers may choose to comply with their resilience-related security duties. It further provides a basis should the Authority need to investigate any telecoms incidents relating to reliability and resilience.

Question 8: 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.

Question 9: 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.

Question 10: Do you have any other comments on the Authority's Draft Resilience Guidance?

4 How to respond to this consultation

4.1 The Authority invites written views and comments on the issues and questions raised in this consultation document. All responses to this proposal should be submitted in writing, clearly marked 'T-062 Telecoms Security', and received by the Authority before 5.00 pm on 17 October 2025. Submissions can be sent by email to info@jcra.je or alternatively in writing to:

Jersey Competition Regulatory Authority
2nd Floor Salisbury House
1-9 Union Street
St Helier
Jersey
JE2 3RF

4.2 It would be helpful if any response includes direct answers to the questions asked in this consultation. It would also help if you can explain why you hold your views and how the Authority's proposals would impact on you, supported by any quantitative or qualitative evidence that you possess.

4.3 Under Authority policy, non-confidential responses to the consultation may be made available on its website (www.jcra.je). Any material that is confidential should be put in a separate annex and clearly marked as such.