Economy

Consultation: Proposed Jersey Telecoms Security Order and Code of Practice

Introduction

This consultation seeks your views on a draft Telecommunications (Security Measures) Order 202- (the draft Order) and Code of Practice for telecoms security.

In particular, it seeks views on:

- Government's proposed approach to securing public electronic communications networks and services as set out in the draft Order and the guidance measures in the draft Code of Practice.
- The Public Telecoms Providers to which Government proposes the draft Oder and draft Code of Practice should apply, as set out in Schedule 1 to the draft Order.
- The approach to phasing in new measures in the draft Code of Practice, so that the recommended compliance timeframes for individual measures set out in the draft Code of Practice account for both security imperatives and proportionate delivery
- The ways in which measures in the draft Code of Practice and the draft Order account for legacy equipment due to be phased out, so that investment in security improvements is distributed appropriately

The draft Order sets out the telecoms security measures that Jersey's Public Telecoms Providers must take once Regulation 8 of the Telecommunications Law (Jersey) Amendment Regulations 2024 (the Amendment Regulations) and the other regulations not yet in force are fully commenced.

The draft Order is accompanied by a draft Code of Practice. Composed of three parts, the draft Code of Practice first explains the role of the Code of Practice within the wider telecoms security framework before explaining the key concepts that underpin the Order to help Public Telecoms Providers carry out the technical measures associated with particular legal requirements in the draft Order. The third part of the draft Code of Practice sets out specific technical guidance measures, as a series of actions that could be taken by Public Telecoms Providers to demonstrate compliance with their legal obligations.

The purpose of the consultation is to obtain the views of stakeholders and the wider community, and to promote discussion on the Order and Code of Practice for telecoms security. Responses will inform our work to finalise the Order and Code of Practice in 2025 and the commencement of the Telecommunications Law (Jersey) Amendment Regulations 2024.

Background

Government of Jersey's Digital Economy Strategy vision is "to unleash a thriving, innovative and inclusive digital future powered by world-class infrastructure and enabling legislation, that delivers sustainable growth for our Island economy."[1]

Jersey's strength as an economy, and its reputation as an international financial services centre and a centre of innovation, is based not only on its laws and high standards but also on the secure and resilient digital connectivity provided by Jersey's telecoms networks and services.

That digital connectivity underpins Jersey's vision of a consistently high-performing, environmentally sustainable and technologically advanced small Island economy. Providing reliable, secure access to the world while sitting at the heart of our Island community, digital connectivity is a key driver of sustainable economic growth and productivity.

Maintaining the security and resilience of Jersey's telecoms networks and services in a rapidly changing world with ever more complex threats and risks is challenging and of crucial importance to Jersey, its businesses and all Islanders.

In recognising the scale and nature of those challenges, the States Assembly agreed in September 2024, to amend the existing the Telecommunications (Jersey) Law 2002[2] in the interests of the security of Jersey and to closely align Jersey's approach to telecommunications security with that of the UK.

Jersey's relationship with the UK is deep and long-standing. Our closest cultural, economic and diplomatic relationships are with the UK, and Jersey looks to the UK Government for its defence and international representation. Our Public Telecoms Providers use UK+44 phone numbers and work closely with UK Public Telecoms Providers and government agencies to maintain the security of our networks and services.

Jersey has developed a telecoms security framework for Jersey's providers of public electronic communications networks and services (PECN / PECS – hereafter referred to as Public Telecoms Providers)[3] that has much in common with the UK's framework introduced by the UK's Telecommunications (Security) Act 2021 (the Act)[4].

Those operating electronic communications networks and providing electronic communications services in Jersey should be aware that a publicly available service is one that is available to anyone who is both willing to pay for it and to abide by the applicable terms and conditions. The term

[1] Digital Economy Strategy. Government of Jersey
[2] https://www.jerseylaw.je/laws/current/l_1_2002
[3] As defined in Article 7 24A of the Telecommunications Law (Jersey) Amendment Regulations 2024
[4] https://www.legislation.gov.uk/ukpga/2021/31/contents

“members of the public” also requires a broad interpretation. Public networks and public services are therefore those that serve business customers and those who serve individual customers.
Jersey remains an independent jurisdiction. The telecoms security elements of the UK’s Act do not apply to Jersey. Ofcom has no telecoms security functions or duties for Jersey under the UK’s Telecommunications Security Act 2021. Jersey’s telecoms security framework including the draft Order and draft Code of Practice are underpinned by Jersey legislation.

Jersey’s framework comprises three layers:

- Security duties on all Public Telecoms Providers. These duties are set out in new Part 5A of the Telecommunications (Jersey) Law 2002, once amended.
- Specific security measures (the Requirements). These are set out in the draft Order and detail the specified measures to be taken in addition to the overarching duties in the Telecommunications (Jersey) Law 2002, once amended.
- Technical guidance. The draft Code of Practice provides detailed guidance to specified Public Telecoms Providers about demonstrating compliance with the duties in the Telecommunications (Jersey) Law 2002, once amended, and the requirements within the draft Order.

The Telecommunications Law (Jersey) Amendment Regulations 2024

Agreed by the States Assembly in September 2024, the Amendment Regulations will, once fully commenced, amend the Telecommunications (Jersey) Law 2002 (the Law) to introduce new duties for providers of public electronic communications networks and services (hereafter referred to as Public Telecoms Providers). Public Telecoms Providers will be required to identify and reduce the risk of security compromises and prepare for the possibility of their occurrence (Article 24K). The Law as amended also places duties on Public Telecoms Providers to prevent, remedy or mitigate any adverse effects of security compromises (Article 24M). These overarching security duties are intended to provide an effective and enduring basis for protecting Public Telecoms Providers.

In addition, the Law as amended provides the Minister for Sustainable Economic Development with new powers to make Orders (Article 24L and Article 24N) and issue Codes of Practice (Article 24O). The proposed Order will set out specific security and resilience measures, providing legal clarity on where Public Telecoms Providers must focus their efforts to secure their public networks and services. An accompanying Code of Practice will provide detailed technical guidance measures to demonstrate how specified Public Telecoms Providers can meet their legal obligations.

A draft Code of Practice has been published alongside this consultation document. The consultation, as required by Regulation 8 (Article 24O), seeks views from Public Telecoms Providers and others who may have an interest or experience in telecoms security, and on the proposals within the draft Code of Practice. The Government is consulting on a draft Order at the same time as consulting on the draft Code of Practice.

The Jersey Competition Regulatory Authority (JCRA) will take on new responsibilities for monitoring and enforcing compliance with the Law and the Order. In doing so, it will take account of the guidance measures within the Code of Practice. The precise ways in which JCRA intends to meet its new duties and exercise its powers and functions will be set out in JCRA's consultation on new procedural guidance. Government and JCRA recognise that improving the security and resilience of Jersey's Public Telecoms Providers is a shared endeavour, and JCRA will seek to work closely with Public Telecoms Providers to meet the objectives of the new security framework.

Developing Jersey's Order and Code of Practice

The content of Jersey's draft Order and draft Code of Practice follow closely the UK's Electronic Communications (Security Measures) Regulations 2022 (ECSM Regulations)[5] and UK's Telecommunications Security Code of Practice (UK Code of Practice)[6], both of which were informed by guidance developed by experts in the National Cyber Security Centre (NCSC). NCSC's guidance was produced following an extensive and detailed analysis of the security of the UK's telecoms sector.

The NCSC provides advice and assistance to Jersey and the other Crown Dependencies as part of existing defence and security arrangements. As such, Government has worked closely with the NCSC to understand the extent to which the NCSC's guidance as set out in the UK's Code of Practice is appropriate and proportionate for Jersey and Jersey's Public Telecoms Providers.

Closely aligned with the UK's Code of Practice, Jersey's draft Code of Practice is, therefore, informed by the guidance provided by NCSC and contains a set of technical and procedural measures designed to ensure that security risks are appropriately managed by Jersey's Public Telecoms Providers. Jersey's Code of Practice takes precedence over the UK's Code of Practice.

NCSC published a summary of its analysis of the risks facing the UK telecoms sector in January 2020, including proposals for applying protections to discrete parts of networks and services, their supply chains and business processes. The UK incorporated NCSC's technical advice into the ECSM Regulations and into the UK's Code of Practice.

Jersey's telecoms security framework applies to Public Telecoms Providers in Jersey. The Government has engaged extensively with Jersey's Public Telecoms Providers throughout the development of the Amendment Regulations, the draft Order and draft Code of Practice.

Given the need for Government to maintain and encourage international relations, development of the draft Order and draft Code of Practice has taken account of the security and resilience policy context in the UK, European Union, United States and elsewhere. It has also taken account of Government's ongoing work to improve the cyber security and resilience of Jersey through the creation of the Jersey Cyber Security Centre underpinned by a proposed Cyber Security (Jersey) Law.

[5] https://www.legislation.gov.uk/uksi/2022/933/contents/made

[6] https://assets.publishing.service.gov.uk/media/6384d09ed3bf7f7eba1f286c/E02781980_Telecommunications_Security_CoP_Accessible.pdf

Contents

Securing Jersey's networks and services

Summary

Government recognises the importance of Jersey's Public Telecoms Providers' networks and services as the key critical national infrastructure (CNI) on which Jersey's economy, Islanders and businesses depend. This consultation makes proposals for an Order that places new obligations on Jersey's Public Telecoms Providers and an accompanying Code of Practice that includes detailed technical guidance demonstrating how Public Telecoms Providers can meet their legal obligations.

Rationale

The rationale for maintaining and improving the security and resilience of Jersey's Public Telecoms Providers is clear. Jersey is dependent on the on-and-off-Island connectivity provided by its Public Telecoms Providers. The threats posed to that vital connectivity have become much clearer as the world has become much less certain.

Government recognises the tensions Jersey's Public Telecoms Providers face between commercial priorities and security concerns, particularly when these impact on investment decisions. It is vital that security and resilience is properly accounted for and concerns addressed as Public Telecoms Providers develop the networks and services Jersey needs.

Risks to network and service security and resilience take a number of forms. In some cases, attackers will seek to exploit vulnerabilities associated with new technologies. The technical characteristics of software-based 5G services will increase the surface area of networks and services open to attack. Alongside technical vulnerabilities, the multiplying number and types of attack increase the risks of a successful compromise where Public Telecoms Providers do not maintain oversight of the most sensitive parts of their network and services. The NCSC has published its extensive security analysis that established the most significant risks to the telecoms sector and continues to publish advice and guidance to Public Telecoms Providers and others.

Jersey's telecoms security framework seeks to embed risk based, good security practices in long-term investment decisions and day-to-day running of Public Telecoms Providers. In doing so, it is a key contributor to Jersey's Strategy for Sustainable Economic Development.

How the measures will work in practice

Once commenced, the changes introduced by the Amendment Regulations will impose new duties on Public Telecoms Providers to address security compromises. The Order will set out specific security and resilience requirements and the accompanying Code of Practice will provide detailed technical guidance measures that demonstrate how Public Telecoms Providers can meet their legal obligations.

The draft Order and draft Code of Practice have been published alongside this consultation. Both are targeted at key risks to Public Telecoms Providers.

The draft Order is designed to mitigate the impact of specific risks in Public Telecoms Providers. The draft Order's requirements are grouped around different network or service features (for example, network architecture or the supply chain) or around the objectives they seek to achieve (for example, ensuring adequate competency of responsible persons). The draft Code of Practice accompanies the draft Order, and is divided into three parts.

The first part explains the purpose of the draft Code of Practice and its position within the new framework. The second part follows the structure of the draft Order. It explains the key concepts underpinning the draft Order, to help Public Telecoms Providers carry out the technical measures associated with particular legal requirements in the draft Order. The third part of the draft Code of Practice sets out specific technical guidance measures, as a series of actions that could be taken by Public Telecoms Providers to demonstrate compliance with their legal obligations.

The individual sections of the draft Order and draft Code of Practice seek to balance the need for effective security and resilience with objectives and actions that are proportionate to risks.

Proportionality and impact of the Order and Code of Practice

Government expects that the Order once made and Code of Practice once in place will have a significant impact on the Public Telecoms Providers to which they apply. The Law as amended requires that any measure specified in the Order must be appropriate and proportionate for the purpose of:

- identifying the risks of security compromises occurring[7];
- reducing the risks of security compromises occurring; and
- preparing for the occurrence of security compromises.[8]

A security compromise includes "anything that compromises the availability, performance or functionality" of networks and services, and "anything that causes signals conveyed by means of the network or service to be lost".[9] Security compromises, therefore, include 'cyber-security type compromises' such as those caused by bad actors, as well as a broad range of other types of impacts on the resilience of networks and services, such as outages caused by external factors (e.g. floods, cable cuts, or power cuts) or internal factors (e.g. hardware failures, operational process errors, or network design flaws).

Jersey's Law as amended is closely aligned with the UK's Act. In developing and proposing an Order and Code of Practice, Government considered the extent to which Jersey's Order and Code of Practice should align with and follow the UK's ECSM Regulations and UK Code of Practice.

[7] Security compromises include network and service outages
[8] Article 8 24L(2)
[9] Article 8 24K (2) https://www.jerseylaw.je/laws/enacted/Pages/RO-052-2024.aspx

The UK's ECSM Regulations and UK's Code of Practice were consulted on in March 2022.[10] As part of that consultation the UK Government produced and published an impact assessment[11] and Business Impact Survey.[12] In September 2022, the UK published its decision about the ECSM Regulations together with a finalised impact assessment.[1314] The ECSM Regulations apply to all UK Public Telecoms Providers who are not micro-entities[15] and the UK Code of Practice[16] published in December 2022 applies to UK Public Telecoms Providers with a relevant turnover of £50m and above in a relevant period. Smaller UK Public Telecoms Providers are not expected to follow the UK Code of Practice.

Jersey's Public Telecoms Providers are significantly smaller in scale and turnover than the largest UK Public Telecoms Providers. Nevertheless:

- Islanders, businesses and CNI depend on the Jersey wide, on-and-off-Island connectivity delivered by Jersey's Public Telecoms Providers. Jersey's Public Telecoms Providers are Jersey's key CNI;
- Jersey is dependent on just four key Public Telecoms Providers for on-and-off-Island connectivity. Two of those four Public Telecoms Providers share network elements and one Public Telecoms Provider makes available wholesale inputs used by the other key Public Telecoms Providers;
- Jersey's Public Telecoms Providers are responsible for delivering a greater range of fixed and mobile services than many similarly sized or larger UK Public Telecoms Providers. Both JT and Sure operate fixed and mobile networks providing services that are similar in nature to the largest UK Public Telecoms Providers who are themselves often part of multinational groups; and
- The UK's ECSM Regulations and UK Code of Practice apply to UK Public Telecoms Providers who are of a similar or smaller scale and turnover than some of Jersey's key Public Telecoms Providers.

Government considers it is of vital importance that the security and resilience of Jersey's connectivity is maintained and that Public Telecoms Providers are capable of responding to evolving threats. Government has engaged with Jersey's key Public Telecoms Providers and UK stakeholders including

[10] https://www.gov.uk/government/consultations/proposal-for-new-telecoms-security-regulations-and-code-of-practice/outcome/proposals-for-new-telecoms-security-regulations-and-code-of-practice-government-response-to-public-consultation#annex-b-list-of-respondents

[11] https://assets.publishing.service.gov.uk/media/62190c11d3bf7f4f0c65c2a6/Consultation_stage_impact_assessment__web_accessible_.pdf

[12] https://assets.publishing.service.gov.uk/media/6239f05ae90e0779a4d55844/Telecommunications_Security_Act_business_impact_survey_-_March_2022__1_.pdf

[13] https://www.gov.uk/government/publications/electronic-communications-security-measures-regulations-and-draft-telecommunications-security-code-of-practice

[14] https://www.legislation.gov.uk/ukia/2022/74/pdfs/ukia_20220074_en.pdf

[15] UK micro-entities are defined in the UK's Companies Act 2006

[16] https://assets.publishing.service.gov.uk/media/6384d09ed3bf7f7eba1f286c/E02781980_Telecommunications_Security_CoP_Accessible.pdf

the NCSC about the extent to which the risk-based approach of the UK's ECSM Regulations and Code of Practice would be appropriate and proportionate for Jersey and its Public Telecoms Providers. Government proposes that it is appropriate and proportionate for Jersey to adopt the risk-based approach taken in the UK's ECSM Regulations and UK Code of Practice.

Given Jersey's reliance on a small number of Public Telecoms Providers who are of similar scale and greater complexity than some UK Public Telecoms Providers, Government is satisfied that the measures included in the UK's ECSM Regulations are appropriate and proportionate as a basis for Jersey's Order. It follows, therefore, that the UK Code of Practice is an appropriate and proportionate basis for Jersey's Code of Practice.

Government has not undertaken a cost benefit analysis for Jersey's draft Order and draft Code of Practice. The remainder of this section sets out a summary of the draft Order and draft Code of Practice.

Network Architecture

The draft Order and guidance measures contained within the draft Code of Practice are intended to ensure networks are securely designed, constructed, where relevant redesigned, developed, and maintained.

Article 3 of the draft Order includes requirements that focus on ensuring Public Telecoms Providers understand the risks of security compromises to network architecture, record those risks, and act to reduce them. The Order requires that Public Telecoms Providers securely maintain networks serving Jersey by ensuring that they can identify security risks and, where necessary, operate their networks without reliance on persons, equipment or stored data located outside the British Islands.

The draft Code of Practice contains measures that support these requirements.

Protection of data and network functions

The requirements and measures about protection of data and network functions are intended to protect the data stored in relation to the operation of networks and services, and secure the functions that allow networks and services to be operated and managed effectively.

Article 4 of the draft Order contains requirements to protect network management workstations from exposure to incoming signals and the wider internet. They also include requirements to monitor and reduce risks from incoming signals to the network or service. In addition, Public Telecoms Providers must act to monitor and reduce the risks of compromise of customer-facing equipment that they supply as part of the public network or service. This includes Public Telecoms Provider-managed equipment such as SIM cards, routers or firewalls. The draft Code of Practice contains measures detailing steps to secure data and network functions, such as the manner in which workstations used to manage the network must be segregated from insecure connections. It also covers encryption of at-rest data and

the correct management of routers and SIMs (including eSIMs).

Protection of certain tools enabling monitoring or analysis

The draft Order and draft Code of Practice contain specific requirements and guidance measures designed to protect tools that enable the monitoring or analysis in real time of the use or operation of Jersey's networks and services, or of the content of signals, against security compromise by hostile state actors.

Article 5 of the draft Order contains requirements to protect monitoring and analysis tools by ensuring that Public Telecoms Providers account for these location-related risks. Schedule 2 of the draft Order lists certain high-risk locations where security capabilities that monitor and analyse Jersey's Public Telecoms Providers' networks and services must not be located. Security capabilities must also not be accessible from those locations. Where Public Telecoms Providers host capabilities in other locations outside of the British Islands, they must identify and reduce the risks of security compromise occurring as a result of monitoring and analysis tools being stored on equipment in those locations.

The draft Order contains measures setting out the steps Public Telecoms Providers can take to identify such risks. These include assessing the risks associated with performing security analysis outside the British Islands and risks related to unauthorised conduct as a result of privileged access being available outside the British Islands.

Monitoring and analysis

The objective of the proposed monitoring and analysis requirements in the draft Order and the guidance measures is to ensure Public Telecoms Providers maintain oversight of access to networks and services in order to reduce the risk of security compromises. Failure to monitor or sufficiently analyse access to a network or service could lead to unauthorised access going unnoticed. This could result in security compromises causing disruption in connectivity for end users and potential data breaches. Undetected access could also enable threat actors[17] to modify access logs.

Article 6 of the draft Order contains requirements that centre on using monitoring and analysis tools to identify and record access to the most sensitive parts of the network or service (defined as 'security critical functions'). This includes securely retaining logs relating to security critical function access for at least 13 months, as well as having systems to ensure Public Telecoms Providers are alerted to and can address unauthorised changes to the most sensitive parts of the network or service. The draft Code of Practice contains measures supporting the requirements, including how analysis should be automated and how logs should be enriched with overlaid data and clearly linked back to specific network equipment or services.

[17] A threat actor is an individual, group, or organization that intentionally attempts to compromise computer systems, networks, or data to cause harm or disruption.

Supply chain

Arrangements between Public Telecoms Providers and their suppliers are central to ensuring Public Telecoms Providers' networks and services are secured effectively.

The objective of the supply chain requirements in the draft Order and the guidance measures is to ensure those arrangements identify and reduce security risks. Exploitation of security vulnerabilities in supply chains could result in security compromises affecting telecoms networks and services. Formalised security relationships between Public Telecoms Providers and their suppliers can help to manage such risks.

Article 7 of the draft Order requires Public Telecoms Providers to put in place appropriate contractual arrangements with their suppliers which, among other things, require suppliers to identify, disclose and reduce risks of security compromises arising from the relationship. They also require Public Telecoms Providers to have written contingency plans that set out what steps will be taken in the event that supply from a third party is interrupted. Where a third party supplier given access to sensitive data is also a Public Telecoms Provider, that Public Telecoms Provider must take the equivalent steps as the primary provider it is supplying. The draft Code of Practice contains measures that enable Public Telecoms Providers to contract securely with suppliers.

Other measures include steps to help agree appropriate shared responsibilities for security between Public Telecoms Providers and their suppliers, and the extension of secure network and service management to third party suppliers.

Prevention of unauthorised access or interference

The draft Order and draft Code of Practice contain specific requirements and guidance measures intended to ensure Public Telecoms Providers understand and control who has the ability to access and make changes to the operation of their networks and services. Failure to manage access to privileged accounts effectively could lead to significant damage being done to a network. For example, if a threat actor gained access to a Public Telecoms Provider's most sensitive management systems they could deny access to legitimate users of such systems or disrupt services provided to end users. Public Telecoms Providers who do not fully understand who is granted access to their network and service management also risk allowing attackers to position themselves for future attacks while remaining unknown to the host Public Telecoms Provider.

Article 8 of the draft Order contains requirements that include applying best practice such as multi-factor authentication and password protections for users who have the ability to make changes to security critical functions. Alongside technical solutions, Public Telecoms Providers should actively approve and be responsible for people's access to administrative accounts, including access to third parties. The draft Code of Practice contains measures that include how particular types of credentials could be protected and how administrative accounts may be structured and used securely.

Preparing for remediation and recovery

The objective of the draft Order and guidance measures on preparing for remediation and recovery is to ensure Public Telecoms Providers are prepared to mitigate the impacts of a security compromise and are able to successfully recover in the event of a compromise. Failures in procedures to remediate or recover networks and services properly could result in Public Telecoms Providers being unable to restore connectivity to end-users in the event of a security compromise. These impacts could be exacerbated if rebuild data is held outside the British Islands and is lost.

Article 9 of the draft Order contains requirements that propose that Public Telecoms Providers hold copies of network and service information that would allow them to rebuild and maintain their operations in the event of a security compromise. A copy of this information must be retained within Jersey. The draft Order also requires that Public Telecoms Providers take steps to recover swiftly and effectively from a compromise. The draft Code of Practice contains further measures that include certain ‘clean up’ steps in the event of a compromise, and cross-references to existing best practice guidance including the NCSC Cyber Assessment Framework to ensure business practices support recovery.

Governance

A key objective of the new security framework is to ensure Public Telecoms Providers understand and manage the risks to their networks and services. Security governance measures will play a central role in ensuring that understanding within telecoms companies. Lack of effective security governance can result in Public Telecoms Providers failing to learn lessons from security incidents and improve their security arrangements accordingly. It can also prevent Public Telecoms Providers from effectively managing tensions between commercial priorities and security concerns, when these impact on costs and investment decisions.

Article 10 of the draft Order includes requirements that assign board-level responsibility (or equivalent) for oversight of new governance processes and effective management of persons responsible for taking security measures within the organisation. The draft Order also sets out how to put an organisational framework in place to manage security incidents from a business process perspective. The draft Code of Practice contains guidance on root-cause analysis and escalation to appropriate governance boards.

Security Reviews

The draft Order and the draft Code of Practice measures relating to security reviews are intended to ensure that Public Telecoms Providers learn about the security of their networks and services so that they are incentivised to make improvements that keep pace with the risks they face. Failure to regularly review the risks of security compromise could result in identifiable security vulnerabilities remaining. Such vulnerabilities could be exploited by threat actors in order to further compromise telecoms networks and services.

Article 11 of the draft Order contains requirements proposing that security reviews of the risks facing networks and services are conducted at least annually. Written assessments would include an assessment of the overall risks of security compromises occurring in the following 12 months. The draft Code of Practice contains specific guidance measures on risk assessment to help ensure it is fit for purpose.

Patches and updates

The objective of this section is to ensure effective use of security patches and upgrades to protect physical and virtual networks and services. The damage caused by failing to upgrade, update or patch physical and virtual infrastructure could be significant. The move to 5G, for example, is underpinned by increased use of software to manage networks and services. This software requires regular security patches and updates to protect it against cyber-attacks (among other things). Public Telecoms Providers that do not carry out, or enable, such patching and updating can leave their networks and services open to known vulnerabilities, which can be exploited by attackers to compromise data or disrupt connectivity.

Article 12 of the draft Order contains requirements standardising best practice, such as rapid patching aimed at - wherever possible - fixing any new vulnerabilities within 14 days of patches becoming available. The draft Code of Practice contains measures that include steps to update networks and services with reference to release dates of relevant updates from suppliers. It also includes steps that could be taken to secure customer premises equipment (such as routers) that are issued, or controlled by, the Public Telecoms Provider.

Competency

The objective of the draft Order and draft Code of Practice measures relating to competency is to ensure that responsible persons understand and manage risks effectively. A lack of skilled and experienced personnel within an organisation can result in poor management of telecoms security risks. This could be exacerbated by failings in structural and organisational culture that is necessary to mitigate such risks.

Article 13 of the draft Order contains requirements that set out the ways in which responsible persons should be competent in fulfilling Public Telecoms Providers' legal security duties and should be given resources to enable them to do so. The draft Code of Practice contains guidance to help ensure effective knowledge and understanding of risks, and appropriate resourcing, including in relation to third party suppliers.

Testing

The draft Order and draft Code of Practice include requirements and guidance measures for testing, which is intended to assess the risks of security compromises to Public Telecoms Providers' networks and services. Lack of testing of systems and processes to uncover potential attack vectors and security vulnerabilities could significantly heighten the risk of security compromises. Relatively low-skilled

commercial hackers may be able to exploit simple security vulnerabilities if they go undetected and unaddressed, resulting in avoidable damage to networks and services and their users.

Article 14 of the draft Order contains requirements mandating the use of testing that simulates, so far as is possible, techniques that might be expected to be used by a person seeking to cause a security compromise. The draft Code of Practice contains measures that include the use of appropriate threat-based penetration testing. It also sets out steps to use testing procedures as part of the management of networks and services.

Assistance

The draft Order and the draft Code of Practice include requirements and guidance measures intended to ensure the sharing of information between Public Telecoms Providers to remedy and mitigate security compromises. This should ensure flexible, agile and swift responses to such compromises when they occur. Poor or slow responses by Public Telecoms Providers contacted for assistance can lead to extended connectivity disruption or data being placed at risk of theft or compromise.

Article 15 of the draft Order contains requirements that ensure Public Telecoms Providers, on request, give assistance to other Public Telecoms Providers in addressing security compromises. The draft Code of Practice contains measures on how Public Telecoms Providers could work together to share information related to particular aspects of their networks (such as international signalling). It also sets out how Public Telecoms Providers could extend assistance provisions to their third-party suppliers. Any such information sharing and assistance remains subject to the Competition (jersey) Law 2005[18] and the requirements and guidance measures do not necessitate breaching that law.

[18] https://www.jerseylaw.je/laws/current/l_6_2005

Alignment of Order and Code of Practice

The requirements and guidance measures set out in the draft Order and draft Code of Practice are intended to represent the most effective way to secure networks and services.

Feedback on the draft Orders and draft Code of Practice will help to ensure the final versions of these requirements and measures are proportionate to the improvements in security they are designed to achieve.

The manner in which the measures in the draft Code of Practice relate to the draft Order is set out in Part 3 of the draft Code of Practice. This ‘mapping’ of guidance measures to the Order’s Articles may be subject to refinement based on the feedback received as part of the consultation process.

Q1. Do you agree that it is appropriate and proportionate for Jersey to adopt the risk-based approach taken in the UK’s ECSM Regulations and UK Code of Practice. If NO, please explain why Government’s proposal to adopt the risk-based approach taken in the UK’s ECSM Regulations and UK Code of Practice are not appropriate and proportionate for Jersey.

Q2. Do you agree that the requirements set out in the draft Order and the guidance measures set out in the draft Code of Practice are an appropriate and proportionate response to address the most pressing risks of a security compromise to Jersey’s Public Telecoms Providers? If NO please set out why, specifically referencing the particular risk of a security compromise, requirements in the draft Order, guidance measures in the draft Code of Practice, and objectives of each section.

Q3. Do you agree it is sufficiently clear which guidance measures in the draft code of practice relate to which Article (or Articles) within the draft Order? If NO please explain why.

Q4. Do you expect the draft Order and draft Code of Practice to have cost impacts on your business? If YES, please provide evidence of the costs

Application of the Order to Jersey's Public Telecoms Providers

Summary

Government proposes that the new security framework should reflect the differences in criticality of Jersey's Public Telecoms Providers. Public Telecoms Providers whose availability and security is critical to Islanders, businesses and Critical National Infrastructure across Jersey are specified in the Order. Those specified Public Telecoms Providers are expected to implement the measures to the timeframes set out in the Code of Practice. Smaller Public Telecoms Providers are not specified in the Order and are not expected to follow the measures set out in the code of practice. Smaller Public Telecoms Providers may choose to implement the measures set out in the Code of Practice.

Government proposes to use market shares reported by JCRA as the basis for deciding which Jersey Public Telecoms Providers should be subject to the Order's requirements.

Rationale

Security measures as set out in the draft Order provide a common set of objectives for Public Telecoms Providers in order to address security risks. The application of the Order and Code of Practice reflect the differences in Jersey's Public Telecoms Providers' networks and services, criticality of the services provided, and their ability to bear the costs of security requirements and measures.

How the measures will work in practice

Government proposes that the draft Order will apply to Jersey's key Public Providers specified in Schedule 2 of the draft Order. Jersey's key Public Telecoms Providers are those for which a security compromise would have the most widespread impact on network and service availability, and the most damaging economic or social effects.

Other Jersey Public Telecoms Providers whose scale means they pose much less risk to Jersey's connectivity are not specified in Schedule 2. The Order will not apply to those other Public Telecoms Providers.

The draft Code of Practice provides guidance measures about how Jersey's Public Telecoms Providers could meet their overarching security duties in the Amended Law and the draft Order. JCRA must take the relevant guidance measures in the finalised Code of Practice as laid before the States Assembly into account when carrying out its relevant functions under the

Telecoms Security Framework (including assessing compliance with the finalised Order when made by the Minister).

Private networks are not in scope of the new security framework introduced by the Amended Law and there is no requirement to follow the technical guidance measures in the draft Code of Practice in relation to the provision of private networks. Providers of private networks may choose to adopt the measures included within the draft Code of Practice.

Basis for specifying Public Telecoms Providers in the Order

Jersey's Telecoms Security Framework seeks to ensure the telecoms networks and services that Islanders, businesses, CNI and wider economy rely on are protected.

The severity of a security compromise could be deemed to be the product of the numbers of customers affected by the loss/disruption of the company's network or service, the importance of the network or service to those customers, and the wider importance to Jersey and its economy. Government believes the most important measure that captures these three factors is Public Telecoms Provider market share of Jersey telecoms market segments.

Market share also reflects the broad ability of a Public Telecoms Provider to bear the financial burden of following the guidance in the Code of Practice. A Public Telecoms Provider with a higher market share will have higher revenue than a Public Telecoms Provider with a lower market share. The Public Telecoms Provider with a higher revenue will have a greater ability to bear the financial burden of following the guidance in the finalised Code of Practice.

It is important the market share information on which Government bases its decision about which Public Telecoms Providers should be specified in the Order and expected to implement measures to the timelines in the Code of Practice is available to, and verifiable by, Government, JCRA and Public Telecoms Providers.

Information about the market shares of Jersey's Public Telecoms Providers in Jersey telecoms market segments is published by JCRA in its annual Telecommunications Statistics and Market Report. Market shares are also set out in JCRA's telecoms market reviews, produced and published in the exercise of its functions and duties. JCRA publishes its annual Telecommunications Statistics and Market Reports and Market Reviews on the JCRA website.[19]

Compiled by Statistics Jersey on behalf of the Guernsey Competition & Regulatory Authority and the JCRA, the Telecommunications Statistics and Market Report 2024 (the Statistics Report) provides information about Jersey's telecoms market segments.[20] Published in June 2025 the Statistics Report for 2024 is based on data submitted by Jersey's licensed telecommunications operators during the first half of 2025. The Statistics Report sets out market shares for JT, Sure, Home Net, Newtel and Airtel in

[19] https://www.jcra.je

[20] Telecommunications Statistics and Market Report 2024. JCRA

Jersey's telecoms market segments for 2019 through to 2024. Market shares for smaller other licensed operators are not reported in the Statistics Report.

JCRA's most recent telecoms market review publication is the Telecoms Market Review – Draft Decision published February 2025 (the Market Review).[21] Produced by JCRA in the discharge of its functions and duties and drawing on information provided by Jersey's Public Telecoms Providers, the Market Review considers the full range of telecoms services provided in Jersey to residential and business customers. The Market Review identifies the following retail services:

- For residential customers: telephony (both fixed and mobile) and broadband; and
- For business customers: telephony (both fixed and mobile), broadband, and managed high capacity services based on dedicated access and end-to-end connections (leased lines).

The Market Review also identifies the wholesale inputs that support the identified retail services.

JCRA's Market Review found JT (Jersey) Limited (JT) to be the largest operator in Jersey and identified Home Net Limited (Homenet), Jersey Airtel Limited (Airtel), Newtel Limited (Newtel) and Sure (Jersey) Limited (Sure) as key market participants. JCRA noted a number of other Jersey licensees offering telecoms services to both consumers and businesses, including Starlink Internet Service Limited, Nitel Limited, and Base Limited T/A Genesis AV.

Proposal for specifying Jersey's Public Telecoms Providers

On the basis of market shares reported in JCRA's Statistics Report and the Market Review, Government proposes the following Public Telecoms Providers should be specified in Schedule 1 of the Order:

- JT (Jersey) Limited (JT), has a central position in Jersey's telecoms markets with market shares reported in retail fixed broadband, fixed voice, leased line and mobile connectivity. JT has market shares reported for the wholesale broadband and leased lines connectivity on which other Jersey telecoms providers depend. Government proposes that JT should be specified in Schedule 1 and be subject to the requirements as set out in the Order.
- Sure (Jersey) Limited (Sure), has market shares reported in Jersey's retail fixed broadband, fixed voice, leased line and mobile connectivity markets. Government proposes that Sure should be specified in Schedule 1 and should be subject to the requirements as set out in the Order.
- Home Net Limited, has market shares reported in Jersey's retail fixed broadband market. Government proposes that Home Net Limited should be specified in Schedule 1 and be subject to the requirements as set out in the Order.
- Newtel Limited, has a reported market share in Jersey's wholesale leased lines market. Newtel also provides the connectivity that Home Net uses to provide fixed broadband and retail leased

[21] Telecoms Market Review Draft Decision JCRA

lines services. Government proposes that Newtel Limited should be specified in Schedule 1 and be subject to the requirements as set out in the Order.

Government does not propose to specify Jersey Airtel Limited (JAL) in Schedule 1 of the Order. JAL's business and therefore market shares in mobile connectivity and retail fixed broadband markets has been acquired by Sure.

Government does not propose to specify in Schedule 1 of the Order, smaller Jersey Public Telecoms Providers for which JCRA do not report market share in a Jersey Telecoms market segment. Smaller providers will not be subject to the requirements set out in the Order.

Ensuring stability for Public Telecoms Providers

Public Telecoms Providers market shares are subject to change over time. New entrants can gain market share and existing Public Telecoms Providers might gain or lose market share, or exit the market. If reported market share is adopted as the metric for specifying Public Telecoms Providers in Schedule 1 of the Order, there must be a mechanism to recognise and reflect those changes. Movement in and out of Schedule 1 on a yearly basis would risk undermining business planning and investment decisions for Public Telecoms Providers. A mechanism must therefore be in place to ensure that Public Telecoms Providers are provided with certainty.

Government proposes that market shares as reported by JCRA are kept under review. Government will amend the Order in the following circumstances:

- Where a telecoms market participant gains market share so that its market share is reported by JCRA in in its annual Statistics Report for a period of two years, the telecoms market participant will be included in Schedule 1 of the Order.
- Where a telecoms market participant loses market share so that its market share is not reported by JCRA in in its annual Statistics Report for a period of two years, the telecoms market participant will be removed from Schedule 1 of the Order.
- Where an telecoms market participant exits the market, the telecoms market participant will be removed from Schedule 1 of the Order.

Government will also consider market share information published in JCRA Market Reviews, where those Market Reviews include market shares for the relevant period under consideration.

Q5. Do you agree that differences between Public Telecoms Providers should be recognised within the Code of Practice through inclusion in Schedule 1 of the Order?

Q6. Do you agree that market share as reported in JCRA's Statistics Report and Market Reviews should be used as the metric for determining which Public Telecoms Providers should be included in Schedule 1 of the Order? If not, are there other metrics that should be used as an alternative or in combination?

Q7. Do you agree with the proposed approach to adding and removing Public Telecoms Providers to Schedule 1? If NO, what alternatives would be most appropriate and why?

Implementation timeframes

Summary

Government expects that some if not all of Jersey's Public Telecoms Providers will have begun to implement a number of the guidance measures set out in the draft Code of Practice.

Some guidance measures set out in the draft Code of Practice will prove more challenging to implement than others. Consequently, Government proposes that the guidance measures in the draft Code of Practice should be phased in over time. Indicative timeframes by which Public Telecoms Providers would be expected to have taken specific measures are set out in the draft Code of Practice.

Rationale

Reflecting differences in security measures

The draft Code of Practice proposes technical guidance measures to help Public Telecoms Providers meet overarching security duties in the Telecoms Law and the draft Order. The guidance measures vary in how costly and complex they will be to implement. A phased approach to implementation takes these differences into account while still achieving the security outcomes intended by the new framework.

Government expects Jersey's key Public Telecoms Providers, JT, Sure, Homenet and Newtel have each been aware of the UK's Regulations and Code of Practice on which Government's proposed Order and Code of Practice are based. That awareness is based on:

- Government's work to bring the UK's draft Telecoms Security Requirements and UK's Code of Practice to the attention of Jersey's Public Telecoms Providers;
- the interactions that Government is aware take place between Jersey's key Public Telecoms Providers and UK Public Telecoms Providers that are subject to the UK's telecoms security framework; and
- the interactions between Jersey key Public Telecoms Providers and the UK's NCSC.

Nevertheless, Jersey's Public Telecoms Providers are likely to be starting from different positions in the development of security arrangements and some Public Telecoms Providers are likely to have made greater progress than others. Government is aware that a number of Jersey's key Public Telecoms Providers have begun work to transform their networks and services. Some of Jersey's key Public Telecoms Providers have made greater progress than others.

Government proposes to take the same approach when proposing implementation timeframes as taken by the UK in the UK's Code of Practice:

- Those measures that are already widespread should have shorter timeframes in the Code of practice, by which Public Telecoms Providers would be expected to have taken relevant measures.
- Measures that require simple changes to formal responsibilities within a business or the creation of access records could potentially be implemented rapidly.
- Those measures that are not so straightforward to implement including those requiring large scale technical solutions or significant resource will require longer timeframes.

How the measures would work in practice

The draft Code of Practice accompanying this consultation sets out a three-phased approach to implementation of security measures, reflecting differences in implementation costs and complexity of those measures.

Public Telecoms Providers specified in Schedule 1 would be expected to:

- implement the most straightforward and least resource intensive measures by 31 March 2027;
- implement more complex and resource intensive measures by 31 March 2029; and
- implement the most complex and resource intensive measures by 31 March 2030.

There may be occasions when Public Telecoms Providers either gain market share, or new providers enter the market and are added to Schedule 1 of the Order. Government propose to apply the same expected implementation timelines to each Public Telecoms Provider specified in Schedule 1, irrespective of how recently they were added to Schedule 1 of the Order.

Enforcement

JCRA has responsibility for monitoring and enforcing the new framework, and will be issuing its own procedural guidance on how this will operate. Timeframes for implementing the guidance measures contained within the draft Code of Practice will serve as guidance on when government expects Public Telecoms Providers to have taken relevant security measures, and JCRA will take account of the final version of the Code of Practice when monitoring compliance with the new framework.

Q8. Do you agree that the guidance measures set out in the draft Code of Practice should be completed in three phases by those Public Telecoms Providers specified in Schedule 1 of the Order: by 31 March 2027, by 31 March 2029, and by 31 March 2030? If NO, please set out what you consider appropriate timelines for expected implementation, making reference to the guidance measures set out in the draft Code of Practice.

Q9. Do you agree that the draft Code of Practice should apply a consistent set of end dates for implementation phases across all Public Telecoms Providers in, regardless of the date they were added to Schedule 1 of the Order?

Legacy networks and services

Summary

Government proposes that the Order and Code of Practice should address the particular challenges of securing 'legacy' equipment and systems, for example, by including requirements and measures to ensure the provision of lifetime support to help maintain security. Government does not suggest including a blanket exemption of such equipment and systems from being covered by the Order or measures in the Code of Practice.

Rationale

Public telecommunications networks have evolved over many decades. While Jersey has a world leading Island-wide full fibre network and is now transitioning to a 5G future, Jersey's Public Telecoms Providers are likely to maintain older technology in their infrastructure. Plans are in place for phasing out legacy equipment and systems as Jersey's Public Telecoms Providers work towards network transformations.

The effective dependency of Public Telecoms Providers on their suppliers should be reflected in procurement processes. A combination of supplier security declarations, contractual commitments to lifetime support and end of support agreement should be included within contracts. This is to ensure equipment is adequately secured even as it approaches the end of its life.

However, where equipment is due to be replaced or phased out, the benefits of investing in new security processes to protect that equipment may be outweighed by the costs. For example, suppliers may have discontinued product lines, or the equipment may have been marginalised within the active network. Public Telecoms Providers may need to weigh investment decisions carefully to account for the possibility that new security approaches may not be appropriate for certain legacy systems and equipment. The draft Order and draft Code of Practice seek to address this issue.

How the measures would work in practice

The draft Order proposes that Public Telecoms Providers ensure their existing networks – which would include legacy elements - are secured. The Order proposes that Public Telecoms Providers take appropriate and proportionate measures "in relation to an existing part of its public electronic communications network, that the part is redesigned and developed in a way that reduces the risks of a security compromise occurring."[22]

The draft Order and draft Code of Practice contain measures to include security support provisions in contractual arrangements between Public Telecoms Providers and their suppliers. Where there are

[22] Draft Order. Article 3(1)(b)

variations in existing contracts from minimum requirements, the draft Code of Practice proposes measures that would identify and mitigate the risks to networks and services.

The challenge of securing legacy networks is also reflected in the proposed measures within the draft Code of Practice. For example it includes measures to restrict unencrypted traffic to legacy systems. Likewise, the draft Code of Practice sets out the need to protect systems that manage network administration by applying ‘zones’ for different activity to ensure the most sensitive aspects of network management are appropriately protected.

Government therefore proposes not to adopt a blanket approach to exempting specific equipment systems as legacy networks. Instead, implementation timelines should take account of large-scale existing change programmes to assist with strategic business planning.

Q10. Do you agree that a blanket approach to exempting specific equipment systems as ‘legacy networks’ is not appropriate given the variation between networks?

Q11. Do you agree with the proposals in the draft Order and draft Code of Practice to address risks arising from legacy systems and equipment? If NO, please explain the reasons for your answer.

How to respond to this consultation

Responses to the question set out within this document (and summarised in Appendix A) can be submitted no later than 3 October 2025:

a. online at gov.je/consultations
b. by email to Economy@gov.je with the subject line FAO Telecoms Security Consultation
c. in writing to:

Telecoms Security Consultation
Department for the Economy
Government of Jersey
Union Street St Helier
Jersey
JE2 3DN

How we will use your information

The information you provide will be processed in compliance with the Data Protection (Jersey) Law 2018 for the purposes of this consultation.[23]

For more information, please read the Department for the Economy's privacy notice.

The Government of Jersey may quote or publish responses to this consultation including (sent to other interested parties on request, sent to the Scrutiny Office, quoted in a published report, reported in the media, published on www.gov.je, listed on a consultation summary etc.) but will not publish the names and addresses of individuals without consent.

Confidential responses will still be included in any summary of statistical information received and views expressed.

Under the Freedom of Information (Jersey) Law 2011, information submitted to this consultation may be released if a Freedom of Information request requires it but no personal data may be released.[24]

Those responding to this consultation should clearly mark responses that are confidential and any part of a response that is confidential.

[23] https://www.jerseylaw.je/laws/enacted/Pages/L-03-2018.aspx
[24] https://www.jerseylaw.je/laws/current/l_17_2011

Appendix A. Consultation questions

Q1. Do you agree that it is appropriate and proportionate for Jersey to adopt the risk-based approach taken in the UK's ECSM Regulations and UK Code of Practice. If NO, please explain why Government's proposal to adopt the risk-based approach taken in the UK's ECSM Regulations and UK Code of Practice are not appropriate and proportionate for Jersey.

Q2. Do you agree that the requirements set out in the draft Order and the guidance measures set out in the draft Code of Practice are an appropriate and proportionate response to address the most pressing risks of a security compromise to Jersey's Public Telecoms Providers? If NO please set out why, specifically referencing the particular risk of a security compromise, requirements in the draft Order, guidance measures in the draft code of practice, and objectives of each section.

Q3. Do you agree it is sufficiently clear which guidance measures in the draft code of practice relate to which Article (or Articles) within the draft Order? If NO please explain why.

Q4. Do you expect the draft Order and draft Code of Practice to have cost impacts on your business? If YES, please provide evidence of the costs

Q5. Do you agree that differences between Public Telecoms Providers should be recognised within the code of practice through inclusion in Schedule 1 of the Order?

Q6. Do you agree that market share as reported in JCRA's Statistics Report and Market Reviews should be used as the metric for determining which Public Telecoms Providers should be included in Schedule 1 of the Order? If not, are there other metrics that should be used as an alternative or in combination?

Q7. Do you agree with the proposed approach to adding and removing Public Telecoms Providers to Schedule 1? If NO, what alternatives would be most appropriate and why?

Q8. Do you agree that the guidance measures set out in the draft code of practice should be completed in three phases by those Public Telecoms Providers specified in Schedule 1 of the Order: by 31 March 2027, by 31 March 2029, and by 31 March 2030? If NO, please set out what you consider appropriate timelines for expected implementation, making reference to the guidance measures set out in the draft code of practice.

Q9. Do you agree that the draft code of practice should apply a consistent set of end dates for implementation phases across all Public Telecoms Providers in, regardless of the date they were added to Schedule 1 of the Order?

Q10. Do you agree that a blanket approach to exempting specific equipment systems as 'legacy networks' is not appropriate given the variation between networks?

Q11. Do you agree with the proposals in the draft Order and draft Code of Practice to address risks arising from legacy systems and equipment? If NO, please explain the reasons for your answer.