Draft Telecoms Security Procedural Guidance

General statement of policy under Article 24Y of the Telecommunications (Jersey) Law 2002

Document No: JCRA 25/20 Publication date: 8 August 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

Document history

Release date	Changes from previous version
08/08/2025	N/A

Contents

1 Overview: Procedural Guidance 1

2 Introduction 3

3 Compliance monitoring 10

4 Reporting security compromises 22

5 Enforcement 36

6 Information sharing 40

1 Overview: Procedural Guidance

Islanders and local organisations depend on reliable communication networks and services to help organise, operate and manage their daily lives, activities and businesses. More than ever, being able to connect with people, other organisations, applications and relevant information is considered highly important – and even critical – to everyday modern life.

At the same time, telecoms systems are becoming more complex in their design and operation, which may lead to an increased likelihood of communication network or service failure. The world is also becoming increasingly fragmented, unpredictable and even threatening, with telecommunications presenting a potential target for malicious actors seeking to disrupt, exploit or harm individuals, organisations and even national economies.

Jersey is not immune from such challenges, which are likely to continue growing and evolving. Recognising this, the Government of Jersey has developed a comprehensive telecoms security framework designed to increase the security and reliability of the Island's communications networks and services. The approach and structure of this framework aligns closely with that operating in the UK and includes a range of legally defined security measures and guidance on how to achieve compliance.

The local telecoms security framework gives the Jersey Competition Regulatory Authority (the **Authority**) legal powers and duties to oversee the telecoms security framework's operation and to work with telecoms providers to ensure its effectiveness. Given the Government of Jersey's decision to align its telecoms security framework closely with that of the UK, the Authority has chosen an approach to its telecoms security functions that aligns closely with that of UK communications regulator Ofcom while taking account of the local context wherever desirable or practical.

Under the telecoms law, the Authority has a duty to publish a statement of its general policy explaining how it will carry out its telecoms security functions under the relevant articles of the amended law.

This document contains that statement of policy, or procedural guidance, issued by the Authority under the amended law. Its purpose is to provide relevant information to public telecoms providers on the Authority's approach to its telecoms security functions under the amended law, and explains the associated procedures that telecoms providers should be aware of and follow, including:

- compliance monitoring;
- reporting the risk and occurrence of security compromises;
- enforcement; and
- information sharing with other public bodies.

The Authority will take the guidance contained in this document and related documents[1] into account when carrying out its telecoms security functions, which include:

- seeking to ensure public telecoms providers comply with their security duties under the amended law which includes carrying out, or commissioning others to carry out, an assessment;
- issuing assessment notices requiring a telecoms provider to comply with a duty;
- directing telecoms providers to explain failure to act in accordance with guidance given by the Minister in a code of practice; and
- enforcing compliance with the security duties, which may include imposing penalties or directing telecoms providers to take interim steps.

This Procedural Guidance sits alongside and complements two other closely related telecoms security framework guidance documents:

(1) Telecoms Security Code of Practice: deals primarily with the measures providers should adopt to protect networks and services from cyber-attacks.

(2) Telecoms Security Resilience Guidance: contains guidance for public telecoms providers that are legally required to design and operate inherently reliable communication networks and services.

The Authority will keep its telecoms security functions under review and may amend and reissue this guidance from time-to-time. Under the amended law and in keeping with its general approach, the Authority will consult on any proposed changes and take reasonable steps to ensure affected telecoms providers are aware of them.

[1] Including the Resilience Guidance

2 Introduction

Jersey's telecoms security framework

2.1 The Telecommunications Law (Jersey) Amending Regulations 2024 (the **Amending Regulations**) amended the Telecommunications (Jersey) Law 2002 (the **Law**) with the aim of increasing the security of Jersey's vital telecoms sector through creating a new telecoms security framework. All providers of public telecoms networks and services (**Providers**) must comply with the legal requirements of this telecoms security framework and certain Providers must further demonstrate their compliance with a range of security measures designed to ensure the effective functioning of Jersey's telecoms critical national infrastructure (CNI) This document is a statement of policy, or procedural guidance (the **Procedural Guidance**), issued under Article 24Y of the Law to explain the Authority's general policy on its telecoms security functions related to the telecoms security framework. The section contains the following content:

- About public telecoms providers
- The new legislative framework
- The Authority's role in the telecoms security framework
- About this Procedural Guidance

About public telecoms providers

PECNs and PECSs

2.2 Before amending, the Law only applied to providers running a telecommunications system. The Amending Regulations created a new telecoms security framework which introduced a range of telecoms security duties that apply to both providers of public electronic communications networks (**PECNs**) and public electronic communications services (**PECSs**).

2.3 These are defined by Article 24A of the Law as being:

> "public electronic communications network" (PECN) means an electronic communications network provided wholly or mainly for the purpose of making electronic communications services available to members of the public.
>
> "public electronic communications service" (PECS) means an electronic communications service that is provided so as to be available for use by members of the public.

Providers of both PECNs and PECSs should be aware of their duties under the Law as amended by the Amending Regulations.

Publicly available service

2.4 For clarity, the Authority considers that "Public Electronic Communications Service" means any electronic communications service that is generally available for use by any and all members of the public who are both willing to pay for it and to accept the associated terms and conditions. A publicly available service is distinguishable from a bespoke service restricted to a limited group of individual and identifiable customers.

2.5 Furthermore, the term members of the public is not limited to residential or small business customers but also corporate or commercial customers including wholesale network connectivity or services provided to other Providers or businesses.

The new legislative framework

2.6 The Amending Regulations introduce the following elements, which are discussed in more detail within this Procedural Guidance:

(a) The overarching security duties set out in Articles 24K and 24M of the Law;

(b) Duties to take specified measures imposed by the Minister by order under Articles 24L and 24N of the Law;

(c) Guidance given by the Minister in codes of practice under Article 24O of the Law;

(d) Duties to report the risk of security compromise to the Authority and to inform users under Article 24S of the Law; and

(e) Duties to report occurrence of security compromises to the Authority under Article 24T of the Law.

The overarching duties set out in the Law

2.7 The Amending Regulations modify the Law to add new security duties for all Providers of public telecoms networks and services in Jersey. Article 24K(1) of the Law sets out the following overarching duty:

> The provider of a public electronic communications network or a public electronic communications service must take measures that are appropriate and proportionate for the purposes of –
>
> (a) identifying the risks of security compromises occurring;
>
> (b) reducing the risks of security compromises occurring; and
>
> (c) preparing for the occurrence of security compromises.

2.8 The term “security compromise”, in relation to a PECN or a PECS, is defined in Article 24K(2) of the Law as:

(a) anything that compromises the availability, performance or functionality of the network or service;

(b) any unauthorised access to, interference with, or exploitation of the network or service, or anything that enables such access, interference or exploitation;

(c) anything that compromises the confidentiality of signals conveyed by means of the network or service;

(d) anything that causes signals conveyed by means of the network or service to be –

(i) lost;

(ii) unintentionally altered; or

(iii) altered otherwise than by or with the permission of the provider of the network or service;

(e) anything that occurs in connection with the network or service and compromises the confidentiality of data stored by electronic means;

(f) anything that occurs in connection with the network or service and causes data stored by electronic means to be –

(i) lost;

(ii) unintentionally altered; or

(iii) altered otherwise than by or with the permission of the person holding the data.

(g) anything that occurs in connection with the network or service and causes a connected security compromise.

2.9 Article 24M of the Law sets out further overarching duties requiring:

(a) The provider of the network or service must take any measures that are appropriate and proportionate for the purpose of preventing adverse effects, on the network or service or otherwise, arising from the security compromise; and

(b) If the security compromise has an adverse effect on the network or service, the provider of the network or service must take any measures that are appropriate and proportionate for the purpose of remedying or mitigating that adverse effect.

Duties to report risk and occurrence of security compromises to the Authority

2.10 Additional to the duties mentioned above, Article 24S of the Law requires all Providers to report certain risks of security compromise to the Authority and Article 24T places a requirement to report certain occurrences of security compromise to the Authority.

Duties to take specified measures imposed by the Minister by Order

2.11 Under Articles 24L and 24N of the Law, the Minister for Sustainable Economic Development (the **Minister**) has powers to provide by Order that a Provider must take specified measures to meet their security duties under Articles 24K and 24M. Under these powers, the Minister issued the Telecommunications (Security Measures) (Jersey) Order(202x) (the **Order**), which came into force on (Day, Month, Year).[2]

2.12 Providers not named in the Order can choose to apply its specific measures and adopt any aspects of the guidance that they consider would be appropriate to secure their networks and services.[3]

Guidance given by the Minister in codes of practice

2.13 Article 24O of the Law also gives the Minister powers to issue codes of practice providing guidance to Providers on compliance with the security measures established by the Order. Under these powers, the Minister issued a Code of Practice (the **Code**) on [Day, Month, Year], setting out guidance for those Providers the Minister has named in the Order as needing to demonstrate compliance with the Code.

2.14 Article 24R of the Law imposes a duty on Providers to explain to the Authority any failure to comply with the Code and gives the Authority powers to require a statement from a Provider in relation to its compliance.

The Authority's role in the telecoms security framework

Introduction

2.15 Under the Law, the Authority has a range of telecoms security functions including several requiring positive approaches and activities, which are introduced in the remainder of this section and explained more fully further on in this Procedural Guidance. These include:

- monitoring and enforcing compliance;
- reporting to the Minister; and
- working with others to enhance the telecoms security framework.

[2] The Government is consulting on draft versions of its Security Measures Order and Code of Practice in Q3 2025, with an expectation to issue final versions in Q1 2026.
[3] In its Draft Code of Practice, the Government states that those specified in the Order will be Providers whose security is most crucial to the effective functioning of Jersey's telecoms CNI.

Monitoring and enforcing compliance

2.16 Article 24V(1) of the Law places a general duty on the Authority to seek to ensure that Providers comply with their security duties. This gives the Authority a clear remit to work with Providers to improve their telecoms security and to monitor compliance with their telecoms security duties.

2.17 The Law gives the Authority powers to monitor and enforce the compliance of Providers with their security duties as specified in Schedule 2 of the Law. In particular, the Law enables the Authority to require Providers to share information considered necessary by the Authority to carry out its telecoms security functions. This includes using its information gathering powers and to issue assessment notices which may include requiring Providers to:

- complete system tests;
- make staff available for interview; and
- permit persons authorised by the Authority to enter a Provider's premises to view information, equipment and observe tests.

Section 3 of the Procedural Guidance contains more information about this.

2.18 Where the Authority has reasonable grounds to believe a Provider is contravening or has contravened a security duty, it may issue a notification of contravention setting out (among other things) the contravention and any remedial action to be taken by the Provider.

2.19 The Authority also has a power to direct Providers to take interim steps to address security gaps during an enforcement process where certain conditions are satisfied, and the Authority determines that it is reasonable to require interim steps pending the completion of enforcement action having regard to the seriousness or likely seriousness of the security compromise. In cases of non-compliance, including where a Provider has not complied with a notification of contravention, the Authority can issue financial penalties. Section 5 of the Procedural Guidance contains more information about this.

Reporting to the Minister and others

2.20 The Authority's telecoms security functions also include certain reporting functions under the new security framework concerning security-related matters.

2.21 Under Article 24U of the Law, the Authority must inform the Minister about certain risks and occurrences of security compromises and provides the power to inform the Minister about the risk or occurrence of other security compromises. The Authority may inform any person or the public (either directly or via a Provider) about the risk or occurrence of security compromises and the technical measures that may be taken in response. Section 4 of the Procedural Guidance contains further information about this.

2.22 Under Article 24Z of the Law, the Authority must provide reports to the Minister for the purpose of allowing the formulation of Jersey's future telecoms security policies. These reports are annual, except the first one, which covers the year in which Article 24Z came into force and the following one. Reports must include the following information for each reporting period:

- the level of compliance with security duties among Providers and the extent to which they have acted in accordance with the Code;
- any reports of risks or occurrences of security compromises received during the reporting period and actions taken by the Authority in response;
- a summary of the telecoms security functions carried out by the Authority during the period, including entering premises, and any particular risks to Jersey's telecommunications networks and services the Authority has become aware of; and
- other information of a kind specified in a direction given by the Minister.

2.23 The Minister, through the States of Jersey, is able to publish these reports or extracts from them.

Working with other public bodies

2.24 Article 24ZG allows the Authority to share information with others about the telecoms security framework in the interests of the security of Jersey or in connection with the prevention, detection or investigation of crime.

2.25 Those others include the Department for the Economy (the **DoE**), through the Minister, as the Government of Jersey policy lead for the telecoms sector; the States of Jersey Police; the Jersey Cyber Security Centre (the **JCSC**), through the Minister, as lead for promoting and improving Jersey's cyber resilience; UK Government departments, including the National Cyber Security Centre (the **NCSC**) as the UK's technical authority for cybersecurity, and other regulators. The Authority will use legal information sharing gateways so that information can be shared where necessary. Further detail on information sharing is set out in section 6 of the Procedural Guidance.

The purpose of and approach to this document

2.26 This document provides general guidance about how the Authority intends carrying out its telecoms security functions under the Law. Its purpose is to establish principles and set expectations for Providers with duties under the Law and who may be obliged to demonstrate compliance. The structural approach closely links the guidance provided with associated provisions under the Law. Wherever appropriate, this guidance document is structured to first highlight the Law's relevant sections and articles, followed by a summary of the Authority's

general policy and approach to allow a fuller understanding of the Authority's chosen approach to its telecoms security functions and emphasise legal obligations placed on Providers.

2.27 In addition to this introduction section, its contents are:

- Section 3: Compliance monitoring
- Section 4: Reporting security compromises
- Section 5: Enforcement
- Section 6: Information sharing

3 Compliance monitoring

Section introduction

3.1 In this section the Authority sets out its approach to monitoring compliance with security duties imposed on Providers under the Law. Its contents include:

- Compliance monitoring principles
- Requirement to demonstrate compliance
- Approach to assessing compliance
- Information-gathering powers
- Testing
- Failure to follow the Code
- Assessments
- Entering premises

3.2 Under Article 24V(1) of the Law, the Authority has a general duty to seek to ensure that Providers comply with their security duties. The Authority will achieve this through adopting a proactive supervisory approach when engaging and working with Providers. This section of the Procedural Guidance sets out the principles behind the Authority's approach to this function, providing general guidance on the compliance monitoring process and steps that may be taken to enforce compliance with Providers' security duties. It also explains how the Authority expects to use its statutory information gathering powers in connection with the telecoms security framework.

Compliance monitoring principles

Duty to seek to ensure compliance

3.3 The Amending Regulations significantly enhance the Law to add substantial additions to regulate security in the Island's telecommunications sector. Within this telecoms security framework, Providers have a greatly expanded range of security duties and the Authority has important new duties and associated powers including seeking to ensure compliance through proactive monitoring and, if necessary, enforcement with legal and regulatory requirements.

3.4 The Authority expects Providers to ensure that they understand and comply with duties placed on them by the telecoms security framework. This means being fully aware of the Law, associated Orders and relevant guidance given by the Minister in the Code and in regulatory

guidance issued by the Authority, including guidance on the resilience of local communications networks and services.[4]

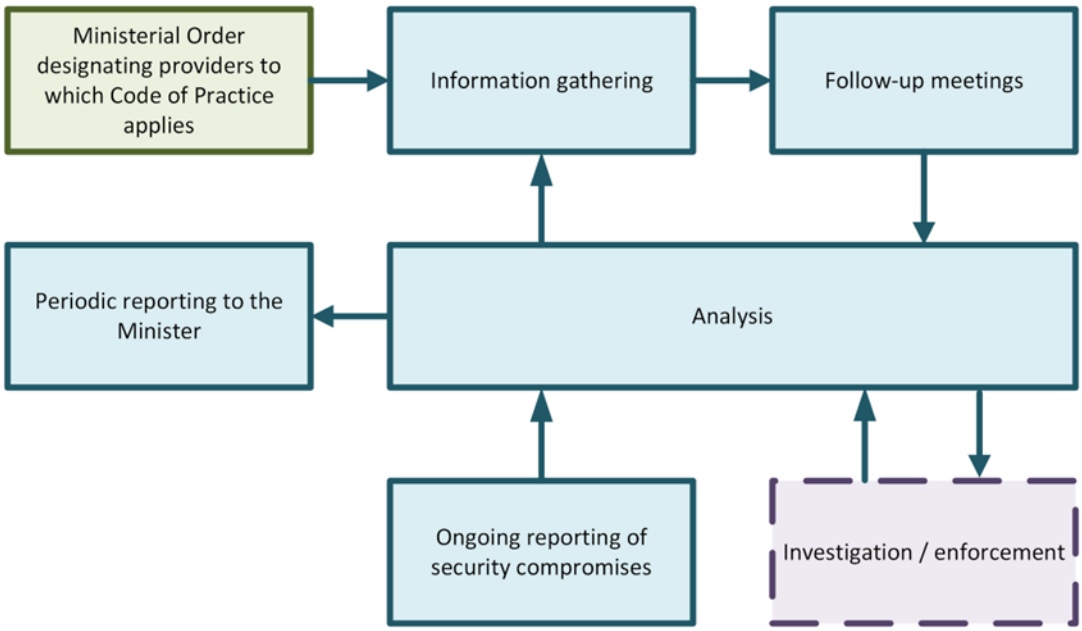
3.5 Article 24V of the Law places a general duty on the Authority to seek to ensure that Providers comply with security duties imposed on them by Articles 24K to 24N, 24S and 24T, which means taking a proactive approach to monitoring and ensuring compliance and carrying out positive enforcement activities if necessary.

Approach to monitoring providers

3.6 While legal duties contained in the Law apply equally to all public telecoms providers, the Authority's compliance monitoring principles apply only to those Providers the Minister has specified in the Order. The rest of this section explains how the Authority intends to approach this monitoring.

3.7 Due to the nature of the telecoms security framework, Providers' implementation of telecoms security measures will evolve and the Authority expects to understand more about their networks, services and compliance approaches over time. For this reason, it sees compliance as an ongoing journey, which will ramp up in line with the phased implementation timeframes set out in the Code. An overview of the Authority's planned approach for the first few years is summarised in Figure 1 below and explained further in this section of the Procedural Guidance.

Figure 1: Compliance monitoring schematic



[4] Reference the Resilience Guidance.

3.8 The Authority understands that the Minister may revise the Order and the Code from time-to-time based on ongoing analysis of the threats and risks faced by Jersey and the need to maintain the security and resilience of the Island's public telecoms networks and services. This may include adding or removing Providers from the list of those identified as having to demonstrate compliance with duties under the telecoms security framework.

A supervisory model

3.9 Through the telecoms security framework, the Minister introduced significant enhancements to help strengthen and protect Jersey's vital communications sector for the benefit of the Island, its economy, organisations and inhabitants. The Authority recognises it is likely to take time for Providers to make the improvements necessary to deliver the benefits intended by the telecoms security framework given the potential scale of change needed.

3.10 The Authority further recognises that threats faced by Providers are continually changing as technologies and threats evolve. Risk management is therefore never complete and requires Providers to develop and maintain a strong internal security culture leading to continuous improvement.

3.11 The telecoms security framework establishes the steps that Providers designated by the Minister must take to achieve compliance with the Law and the Order. Through its supervisory model, the Authority will initially monitor progress that each Provider is making towards implementing appropriate organisational and technical measures with sufficient pace, as they continue to work towards full compliance. Where the Authority finds areas of concern, it will seek to work with Providers to ensure appropriate and proportionate measures are implemented in accordance with the telecoms security framework. The Authority expects that this collaborative approach will foster more compliant behaviours and reduce the volume of breaches under the Law, as well as reducing the need for regulatory investigations. As necessary, the Authority will also stand ready to engage its suite of enforcement powers with the approach to enforcement set out in Section 5 of the Procedural Guidance.

Gathering information to assess compliance

Legal framework

3.12 Article 24ZC of the Law provides the Authority with broad powers to gather any information it considers necessary to carry out its functions under the Law, including:

(a) To assess whether a Provider is complying or has complied with its telecoms security duties under Articles 24K to 24N, 24R and 24T and issuing appropriate notices;

(b) To prepare a report to the Minister under Article 24Z; and

(c) For the purpose of assessing the risk of a security compromise occurring in relation to a PECN or PECS;

(d) To facilitate the provision of security information by requiring a Provider:

i. to produce, generate or obtain information;

ii. to collect or retain information that the person would not otherwise collect or retain; or

iii. to process, collate or analyse any information held by the person (including information the person has been required to collect or retain) for the purpose of producing or generating information to be provided to the Authority.

3.13 The security information that the Authority can require can include information under Article 24ZC(4)(e) concerning future developments of a PECN or PECS that could have an impact on the security of the network or service.

The Authority's general policy for assessing compliance

3.14 The Authority intends relying primarily on statutory information requests issued under 24ZC of the Law (**Information Request Notices**) to build its initial understanding of each Provider's compliance with the telecoms security duties, which includes any adherence to the Code. The Authority has a wide range of other powers that it can use where necessary to collect additional information about compliance, such as assessment notices issued under Schedule 2, Part 2, 1(1-3) of the Law and notifications directing a Provider to give a statement to the Authority under Article 24R explaining whether they have failed to act in accordance with guidance given by the Minister in the Code, and why.

3.15 The Authority recognises that the systematic use of Information Request Notices within the telecoms security framework will be a mostly new process for Providers. For this reason, the Authority would normally expect to send notices in draft form for review and comment where timescales allow and it is appropriate to do so, before sending a final notice. The Authority also expects to refine information requested through the Information Request Notice process as it gains experience of the process, such as the level of detail required or the extent of information gathered in a notice.

3.16 The Authority recognises that the process of building its understanding of compliance is a new practice for both itself and Providers and that the telecoms security framework requirements covered by the Order and the Code may require Providers to plan and implement considerable changes to the delivery of their networks and services. The Authority has designed its compliance monitoring regime based on this, employing a multi-stage approach through which it expects Providers to demonstrate their compliance with the Security Measures over several tranches and in line with the Minister's timeframe established in the Code. The Authority may

also refine the compliance monitoring process based on experience gained through implementation and operation.

3.17 An initial step on the compliance monitoring process will be for the Authority to build a comprehensive understanding of Providers' networks and services to establish those in scope of the telecoms security framework, and the various functions and assets they comprise. This will provide the Authority with a clear understanding of each Provider's full range of "security critical functions" (as defined in the Order), and which of these are "network oversight functions" (as defined in the Code). Based on this understanding, the Authority will be able to assess whether the Provider is taking appropriate measures to protect each of them.

3.18 Concurrently with activities to understand the scope of networks and services, the Authority will request information to understand the measures each Provider has in place in order to meet its obligations under the Law and the Order. The Law requires the Authority to take relevant provisions of the Code into account when assessing compliance, so information requested will be primarily intended to help establish:

(i) the extent to which measures the Provider has in place, or is planning to put in place, align with those in the Code; and

(ii) any alternative or additional measures which Providers might take to comply with their security framework duties.

Alongside asking about the measures a Provider has in place, the Authority may also ask for relevant documentation or other information describing or demonstrating a measure.

3.19 The Authority expects to use Information Request Notices issued directly to Providers to gather most of the information needed to assess compliance with the telecoms security framework obligations. However, Article 24ZC(1) of the Law also allows the Authority to gather information from other relevant persons, which include:

(i) other public communications Providers;

(ii) persons supplying electronic communication apparatus;

(iii) persons making associated facilities available to others; and

(iv) any other person the Authority believes relevant.

3.20 The Authority may choose to use other powers under the Law if it has concerns that Information Request Notices issued as part of its regular compliance monitoring programme, both to Providers and others, are not providing the required information. These powers include:

(i) the Authority's power under Article 24R of the Law to direct Providers to explain any failure to act in accordance with guidance given by the Minister in the Code; and

(ii) The Authority's powers under Schedule 2, Part 1 to give assessment notices (which are covered in the Procedural Guidance below).

3.21 The Authority recognises that demonstrating complete compliance with telecoms security framework obligations from the outset may be challenging for Providers, given its scope and scale. The Code sets out several dates spanning 2027 to 2030, reflecting the Minister's expected timescales for implementing the different measures specified by the Order. The Authority will put in place a progressive compliance monitoring programme, which includes several rounds of information gathering and assessment with each building toward gaining a complete understanding of a Provider's compliance with security measures required by the Order and based on the obligations and timeline contained in the Code. Through this programme, the Authority will track progress and receive early warnings of any potential compliance concerns.

The Authority's information-gathering programme

Approach and timetable

3.22 Each round of information requests of the Authority's information gathering programme will contain the following steps:

Step 1	The Authority will draft the Information Request Notice and normally share with the Provider for review and comment.
Step 2	Accommodating any relevant comments received, the Authority will issue the statutory Information Request Notice to the Provider.
Step 3	The Provider responds to the Information Request Notice providing the required information in the specified format and by the stated time.
Step 4	The Authority will review the information received and may follow-up with clarification requirements through informal meetings and correspondence with the Provider or through further Information Request Notices.

The Authority expects to begin its first round of information requests within three months of starting its duties under the telecoms security framework, to cover gaining understanding of Providers' networks and services and compliance against a first round of security measures. The Authority plans to release subsequent information requests at nine month intervals with around six requests expected to cover all Code measures. The intention behind the multiple requests is to help keep the burden imposed by each manageable.

3.23 The above approach may need amending dependent on many factors, such as:

- any specific compliance concerns arising, for example, from reported security compromises or previously received information;
- any new threats, and associated security measures, that arise; or
- any concerns about the information received, such as in relation to its completeness, accuracy or quality.

Follow up meetings

3.24 The Authority may need to improve its understanding of a Provider's compliance through seeking clarification on information received or request additional information beyond that included in a written response to an Information Request Notice. Where appropriate, the Authority expects to do this via correspondence and meetings, with Providers receiving reasonable notice of any such meetings. The Authority will aim to limit them to those it considers necessary to develop a sufficiently thorough understanding of the measures taken by Providers to comply with their security duties.

Handling sensitive data

3.25 The Authority will use an appropriate platform to securely receive, process and store confidential information received from Providers under the telecoms security framework. Providers will receive operational arrangements for supplying sensitive data when the Authority issues Information Request Notices.

Information sharing

3.26 The Authority provides information on its approach to sharing information relating to the telecoms security framework, including information received through its compliance monitoring programme, in Section 6 of the Procedural Guidance.

Testing

Introduction

3.27 The Order requires Providers to carry out tests at regular intervals designed to identify the risk of security compromises. These tests must involve simulating techniques that might be used by a person seeking to cause a security compromise. The Code provides further information to help Providers understand testing requirements.

3.28 In general, the Authority expects Providers to be fully aware of and comply with their testing obligations under the Order. This part of the Procedural Guidance provides further information on how the Authority expects to use its powers under Schedule 2, Part 1 of the Law to monitor compliance.

Relevant legal framework

3.29 Under Schedule 2, Part 1 of the Law, the Authority has the power to carry out, or commission others to carry out, an assessment of whether a Provider is complying with (or has complied with) the security duties under the Law. Schedule 2, Part 1, 1(3) also provides the Authority with power to give Providers an assessment notice for the purpose of carrying out an assessment. In particular, these powers include requiring a Provider to:

- carry out specified tests or tests of a specified description in relation to the network or service;
- make arrangements of a specified description for another person to carry out specified tests or tests of a specified description in relation to the network or service;

3.30 A test required by an assessment notice may include tests which risk causing a security compromise, or loss to a person or damage to property, but only if the test uses techniques which might be expected to be used by a person seeking to cause a security compromise.

The Authority's general policy

Testing requirements

3.31 The Code explains the purpose of testing, or "red team" exercising, is to verify the security defences of the network and identify any security weaknesses prior to any potential attackers. For this reason, it is essential that the testing simulates, so far as possible, real world attacks. The Code provides guidance on the criteria any test should have in place to achieve this.

3.32 The Authority expects Providers to voluntarily establish a testing regime that meets the criteria set out in the Code and referred to above. In particular, testing should simulate an advanced attack against a Provider's critical infrastructure and assets, usually drawing from four different scenarios:

- attack from the Internet;
- an attacker with insider privileges;
- an attack through a 3rd party service provider; and
- an attack against physical infrastructure (if applicable).

3.33 The Authority may require Providers to report on their structured testing regime and results of testing and, based on results, may require them to develop and share a mitigation plan to address the findings and works.

Failure to follow the Code

Relevant legal framework

3.34 Failure to act in accordance with a provision of the Code does not of itself make a Provider liable to legal proceedings. However, under Article 24R(1) the Authority may notify a Provider where it has reasonable grounds for suspecting that the Provider is failing or has failed to act in accordance with a Code provision. The notification must:

- set out (i) the relevant provision(s) of the Code and (ii) the respects in which the Provider is suspected to be failing, or to have failed, to act in accordance with such provision(s); and
- direct the Provider to give a statement in response.

3.35 In its statement, the Provider must confirm whether or not it is failing, or has failed, to act in accordance with a provision of the Code and explain the reasons for its response.

The Authority's general policy

3.36 In the first instance, it is for Providers themselves to determine how their security duties affect their activities and take any necessary measures in order to comply with them. Therefore, the Authority expects Providers to take proactive steps to meet their regulatory obligations.

3.37 As explained above, the Authority intends relying primarily on statutory Information Request Notices as the basis of its compliance monitoring framework. As part of this, the Authority will ask Providers for information to assess whether they are complying with their security duties, taking into account any relevant provisions set out in the Code. Where this or other information gives the Authority reasonable grounds to suspect Providers are not acting in accordance with the Code, it may use its power under Article 24R. The Authority will use the information provided to inform its compliance assessments and when considering any subsequent enforcement action.

3.38 In practice, the Authority expects Providers to engage constructively with its routine monitoring processes and provide a clear picture of the steps they are taking towards compliance when providing information in response to Information Request Notices. Therefore, the Authority only anticipates using its power under Article 24R where it considers that a clear statement from a Provider of the type required under 24R is necessary for the Authority to consider whether further escalation might be appropriate. Any use of this power will take into account the implementation timelines attached to provisions in the Code.

Assessments

Relevant legal framework

Duties specified in the Authority's assessment notices

3.39 Schedule 2, Part 1 of the Law sets out the Authority's powers to assess Providers' compliance with their security duties and gives the Authority the power to carry out, or commission others

to carry out, an assessment of whether a Provider is complying with (or has complied with) the security duties in Articles 24K to 24N, 24S and 24T. Providers have a duty to cooperate with an assessment and are also required to pay the Authority's reasonably incurred costs in connection with the assessment.

3.40 Schedule 2, Part 1, 1(3) provides the Authority with the power to give Providers an assessment notice for the purpose of carrying out an assessment. It sets out what an assessment notice may require a Provider to do and may specifically require a Provider to:

- carry out specified tests (or tests of a specified description) in relation to the network or service (covered earlier in this section);
- make arrangements for another person to carry out specified tests (or tests of a specified description) in relation to the network or service;
- make people available for interview that must be those of a specified description who are involved in the provision of the network or service and must not exceed the number who are willing to be interviewed; and
- permit authorised persons to enter specified premises for various purposes (this power of entry is discussed in more detail in the "Power to enter premises" part of the Procedural Guidance below).

3.41 Schedule 2, Part 1, 2 allows the Authority to issue an assessment notice which requires that the Provider must comply with a duty urgently, in which case the usual rules regarding the timeframe for complying with a duty and how this may be affected by an appeal do not apply. Schedule 2, Part 1, 3 also makes provision for a Provider to apply to the court for an order that the duty in such an urgent notice does not need to be complied with urgently, and/or a change to the time at which (or period within which) the duty must be complied with.

The Authority's general policy

3.42 As noted above, there may be circumstances where the use of the Authority's broader suite of powers under the Law, such as the power to issue assessment notices, is necessary. These powers allow for a range of activities, such as carrying out tests on a network or service, interviewing staff, visiting premises and observing or inspecting operations, documents and information.

3.43 While the Authority expects to gather the majority of information through its routine monitoring using Information Request Notices, it may, in some circumstances, decide it is appropriate to use an assessment notice to inform the Authority's assessment of a Provider's compliance with their security duties.

3.44 The Authority recognises that complying with an assessment notice may require more substantial effort or additional costs for Providers than responding to receiving Information Request Notices or providing a statement in response to one.

3.45 Where appropriate, the Authority may also use assessment notices to inform its enforcement activity and reminds that Providers have a duty to cooperate with an assessment under the Law and holds the view that this would include not doing anything to disrupt an assessment, such as destroying documents to which access is sought or interfering with testing required by an assessment notice. The Authority has powers to enforce any breach of this duty of co-operation under Schedule 2, Part 2, 8(3).

Entering premises

Legal framework

Duties specified in the Authority's assessment notices

3.46 As part of the Authority's powers to assess Providers' compliance with their security duties, Schedule 2 permits it to issue assessment notices that require Providers to do various things, which include permitting an employee of the Authority or other person authorised by the Authority (an "authorised person") to enter non-domestic premises for various purposes. Specifically:

- to observe any relevant operations taking place;
- to direct an authorised person to relevant equipment or other material or documents of a specified description;
- to assist an authorised person to view information of a specified description that is capable of being viewed using equipment on the premises;
- to comply with a request from an authorised person for a copy of the documents to which the person is directed and the information the person is assisted to view;
- to permit an authorised person to inspect or examine the documents, information, equipment or material to which the person is directed or which the person is assisted to view; and
- to provide an authorised person with an explanation of such documents, information, equipment or material.

Referring to the Authority's exercise of its power of entry in its security reports

3.47 Article 24Z (5)(g) of the Law requires the Authority to include a statement which sets out the number of occasions on which premises have been entered in its annual report to the Minister.

The Authority's general policy

3.48 In exercising its powers of entry, the Authority expects to have regard to any relevant legislation or guidance provided in this area.

3.49 The Authority will set out the number of times premises have been entered during the course of each financial year in its annual report.

4 Reporting security compromises

Introduction

4.1 Under the Law, Providers have a duty to report the risk and occurrence of security compromises, which encompasses both resilience and cyber related incidents. This requires them to notify users and the Authority about the significant risk of security compromise and to report security compromises to the Authority. This section explains the Authority's expectations of Providers in relation to these duties and contains the following contents:

- Informing of the significant risk of a security compromise; and
- Reporting the occurrence of a security compromise.

Informing of the significant risk of security compromise

Relevant legal framework

4.2 Under Article 24S of the Law, Providers must take reasonable and proportionate steps to inform users who may be adversely affected by any significant risk of security compromise of a PECN or PECS. The relevant information to provide users is:

- the existence of the risk;
- the nature of the security compromise;
- the technical measures that it may be reasonably practicable for such users to take in response to prevent, remedy or mitigate the adverse effect that the security compromise would have on them; and
- the name and contact details of a person who may provide further information.

4.3 Under Article 24S(2)(b) of the Law Telecoms Providers must also notify and provide the Authority with the same relevant information relating to the risk of security compromise.

4.4 Under Article 24S(4) of the Law, the Minister may subsequently by order specify a minimum time by which Providers must take the steps to bring the relevant information to the attention of affected persons and the Authority.

The Authority's general policy on the risk of security compromise

Duty to inform users

4.5 The duty to inform users of the risk of a security compromise applies where there is both:

(a) A "significant risk of a security compromise occurring"; and

(b) Where such a security compromise may adversely affect users.

Providers are likely to be aware of many potential vulnerabilities within their networks and services, most of which are unlikely to result in an actual security compromise, or even if they did, they would be unlikely to have an adverse effect on users. Therefore, where Providers have reasonable grounds for believing that a vulnerability within the network or service is unlikely to result in an actual security compromise, or even if it did, it would be unlikely to have an adverse effect on users, the Authority would not expect users to be informed of such matters under Article 24S.

4.6 Providers should consider a number of factors when determining whether to inform users about a significant risk of security compromise, including:

- Does the risk arise from a vulnerability for which there is a known means to exploit and/or any known active exploitation?
- How difficult would it be to exploit any vulnerability that gives rise to the risk?
- Are there any actors likely to be able to exploit any related vulnerability and likely to do so in a way which adversely affects users of the network or service?

4.7 If the Provider determines there is indeed a significant risk of a security compromise occurring, and that users may be adversely affected by this, the Provider must take steps to inform relevant users. What will be required by Article 24S will depend on what is reasonable and proportionate in the circumstances for the purpose of bringing the relevant information to the attention of those users that may be adversely affected. Generally, there are two broad categories as to the approach that might be adopted:

- Direct contact. This could, for example, be via an email, letter or telephone call to each potentially affected user of the network or service; and
- Indirect contact. This could, for example, involve publishing a notice on the Provider's website in a location that is well signposted.

4.8 Factors which the Authority considers are likely to make direct contact more appropriate include:

- Where the security compromise could be reasonably expected to cause significant harm to the users;
- Where there are measures that could reasonably be taken by a typical user which would significantly reduce or eliminate a serious adverse effect from the security compromise;
- Where no such measures exist, but the user could mitigate the risk to themselves by making a decision to move to an alternative Provider.

4.9 Providers must ensure that direct contact takes into consideration vulnerable customers' preferences and requirements for direct contact, and not rely on a one size fits all communication approach. The Authority considers vulnerable customers to be users that the Provider has been informed of or should otherwise reasonably be aware may be vulnerable due to circumstances such as age, physical or learning disability, physical or mental illness, low literacy or communications difficulties.

Duty to notify the Authority

4.10 When communicating with users about the significant risk of a security compromise, Providers must also notify the Authority of the relevant information being shared. Information on how and what to report to the Authority in these circumstances is shown below, along with further details.

How to report a significant risk of compromise

4.11 Providers should submit the relevant information about a significant risk of a security compromise using a secure communication method specified by the Authority at the same time they communicate with users.

4.12 Providers may also choose to provide the Authority with further supplementary information about the risk if they consider appropriate for helping the Authority better understand relevant circumstances or details. Providers sharing any supplementary information should use the secure communication method specified by the Authority for this purpose.

Data required

4.13 Each significant risk of compromise report should include the relevant information being shared with users, which is:

- the existence of the risk;
- the nature of the security compromise;
- the technical measures that it may be reasonably practicable for such users to take in response to prevent, remedy or mitigate the adverse effect that the security compromise would have on them; and
- the name and contact details of a person who may provide further information.

Follow-up actions or requirements in response to a significant risk of security compromise report

4.14 After receiving a significant risk of security compromise report, the Authority may contact the Provider to request further details. These could include further information on the nature of the risk and the Provider's actual/planned response.

4.15 The Authority expects Providers to manage any significant risk of security compromise appropriately under duties imposed by the Law. Should the Authority consider the Provider has not handled a significant risk of compromise to its satisfaction, the Authority may decide to use its assessment and enforcement powers set out in Schedule 2 of the Law to address any possible shortcomings.

Information sharing

4.16 The Authority provides information on its approach to sharing information relating to the telecoms security framework, including information received through reports of significant risks of security compromise, in Section 6 of the Procedural Guidance.

Reporting the occurrence of security compromise

Legal framework

4.17 Article 24T(1) of the Law requires Providers to inform the Authority as soon as reasonably practicable of any security compromise that:

- has a significant effect on the operation of the network or service; or
- involves unauthorised access to, interference with or exploitation of the network or service so that a person is put in a position to bring about a further security compromise that would have a significant effect on the operation of the network or service.

4.18 Article 24T(2) of the Law requires Providers to take account of a number of factors in determining whether the effect that a security compromise has, or would have, on the operation of a network or service is significant for the purposes of complying with their reporting obligation. These factors are:

(a) The length of the period during which the operation of the network or service is or would be affected;

(b) The number of persons who use the network or service that are or would be affected by the effect on the operation of the network or service;

(c) The size and location of the geographical area within which persons who use the network or service are or would be affected by the effect on the operation of the network or service; and

(d) The extent to which activities of persons who use the network or service are or would be affected by the effect on the operation of the network or service.

4.19 Under Article 24T(3) of the Law, the Minister may by order specify a minimum time by when Providers take steps to inform the Authority of any reportable occurrence of security compromise.

The Authority's general policy

4.20 Article 24T of the Law places a requirement on all Providers of PECNs and PECSs to report security compromises to the Authority. This supersedes any existing reporting requirements established between the Authority and Providers or stated in any previous guidance or agreements and applies to all Providers whether they are obliged to demonstrate compliance with the telecoms security framework or not.

4.21 The Authority recognises this incident reporting requirement and the criteria and time limits established in this section of the Procedural Guidance are likely to involve an increased level of reporting activity by Providers and potential subsequent engagement with the Authority to understand the nature and impact of security compromises. However, the Minister has responded to a changing security situation by introducing the Amending Regulations, and therefore the Authority expects Providers to understand and comply with incident reporting requirements.

4.22 Under Article 24K(2)(a) of the Law, security compromises required to be reported to the Authority include "anything that compromises the availability, performance or functionality of the network or service". The Authority expects the majority of these to be network or services outages arising from equipment or process failures or similar, and causing "availability" or "resilience" incidents.

4.23 The definition of security compromise in Article 24K(2) of the Law includes a number of situations other than network or service outages, many of which are typically associated with cyber-security incidents. In particular, those described in Article 24K(2)(b)-(f), which cover aspects such as confidentiality and integrity. This means that any security compromises, including those related to cyber-security incidents, which meet the criteria in Article 24T must be reported in addition to the reporting of network or service outages. Examples of confidentiality and integrity related incidents include any instances where an attacker has infiltrated the network, is using the network for their own purposes or is stealing data. Some examples of the type of incidents that would likely be reportable are found in Table 3 below.

4.24 The Authority notes in particular that Article 24T(1)(b) states that the following is also reportable:

> "any security compromise within Article 24K(2)(b) that puts any person in a position to be able to bring about a further security compromise that would have a significant effect on the operation of the network or service."

4.25 Therefore, any event that puts any person in a position, however briefly, to be able to bring about a further security compromise that would have a significant effect, must also be reported

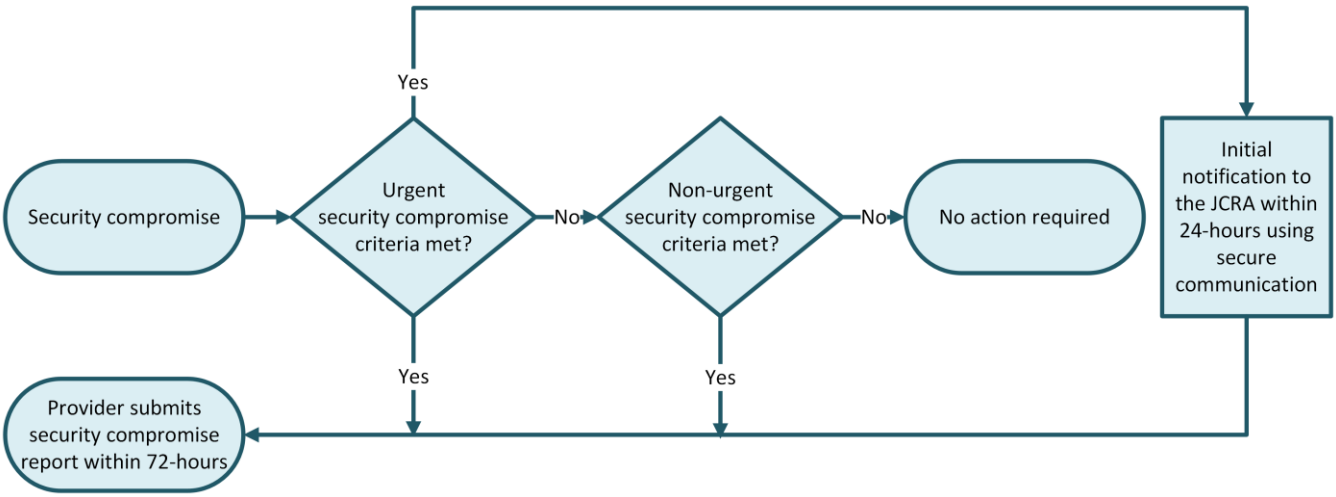
(even if the defences put in place by the Provider make a further attack unlikely to succeed). An example of such a situation would be where an attacker had gained access to a system, which they could have used to mount a further attack and cause significant effect.

4.26 The remainder of this section sets out further guidance for Providers on:

- Which security compromises to report, through qualitative criteria and numerical thresholds for what constitutes a reportable security compromise;
- When to report, with guidance on expected reporting timeframes for urgent and non-urgent security compromises; and
- How to report security compromises.

4.27 Figure 2 below illustrates the end to end process for reporting security compromises.

Figure 2: Reporting security compromises schematic



Which security compromises to report

4.28 The qualitative criteria and numerical thresholds set out below, which have been developed taking into account the factors listed in Article 24T(2) of the Law, explains the Authority's view of which security compromises are likely to be significant and should therefore be reported to the Authority. If any one of the criteria or thresholds is met, the Provider should submit a security compromise report. The Authority has the power to take enforcement action where this does not happen in accordance with the statutory requirements.

4.29 Reportable security compromises are as follows:

- Any security compromises impacting service availability, which meet the thresholds set out in Table 1 or Table 2 below;

- Any security compromises affecting networks or services involved in connecting emergency calls (e.g. Call Handling Agent platforms, emergency call routing, etc.) and leading to a reduction in the usual ability to answer or correctly route calls;
- Any security compromises that the Provider is aware of that have a link to a potential loss of life;
- Any security compromises involving significant cyber security breaches (see illustrative examples in Table 3 below);
- Any security compromises reported to other Government of Jersey agencies or departments;
- Any security compromises that Providers are aware of being reported in the media (Jersey, UK or trade news sources).

Table 1: Fixed network numerical thresholds

Network/service type	Minimum number of end users affected[1]	Minimum duration of service loss or major disruption
Fixed network providing access to the emergency services	100	1 hour
Fixed network providing access to the emergency services	1,000	Any duration
Fixed voice or data service/network offered to retail customers	100 or 25%[2]	8 hours
Fixed voice or data service/network offered to retail customers	1,000	1 hour

Notes on Table 1:

1. *A user is affected if the main functions of a network or service are not available to them due to the security compromise.*
2. *This threshold should be interpreted as either 1,000 end users or 25% of the Provider's total number of end users on the affected service, whichever is the lowest number.*

Table 2: Mobile network numerical thresholds

Network/service type	Minimum number of end users affected[1]	Minimum duration of service loss or major disruption
Mobile network providing access to the emergency services	100	1 hour
Mobile network providing access to the emergency services[2]	1,000	Any duration
MVNO voice or data service/network offered to retail customers[3]	25%[2]	8 hours
MNO voice or data service/network offered to retail customers	1,000	1 hour

Notes on Table 2:

1. *A user is affected if the main functions of a network or service are not available to them due to the security compromise.*
2. *A mobile virtual network operator (MVNO) should report security compromises affecting its end users, even where security compromises are the result of a failure in its host mobile network operator's (MNO's) network. In this case, the third party's details should be provided.*
3. *This threshold should be interpreted as 25% of the Provider's total number of end users on the affected service*.

4.30 For illustrative purposes, Table 3 below sets out a list of examples of cyber-security compromises which the Authority expects would have been reportable under Article 24T of the Law, if suffered by a Provider. It is non-exhaustive, and Providers should monitor for other categories of cyber-security compromise and report to the Authority for information and consideration. The Authority reminds Providers that resilience incidents are also reportable.

Table 3: Examples of cyber-security compromises

Category	Explanation
Supply chain compromise	Products used in a Provider's network/service are compromised, as a result of an attack on the supplier.
Successful Exploitation of Vulnerability	An external attacker carrying out a targeted internet-based attack.
Physical attacks	Attacks with a starting point in physical assets such as a base station or street cabinet. This could lead to loss of service or give the attacker physical or logical access to security critical functions (SCFs) or network oversight functions (NOFs).
Managed service-based attack	An external attack via a Managed Service Provider (MSP) used by the Provider. This could be via a malicious employee from the MSP or because the MSP has had a security compromise, that facilitates an attack into a Provider.
Malicious insider attack	A malicious attack that has been perpetrated by an insider on the company network or by an insider who has been influenced by an external threat actor.
Ransomware	Either a targeted or "random" attack that encrypts data for ransom and/or extracts data for ransom.
Internet routing protocol abuse	When attackers reroute internet traffic (maliciously, or due to misconfiguration). Examples include BGP hijacking and DNS poisoning.
Security misconfiguration	Systems are not correctly/insufficiently secured leaving an exploitable loophole/vulnerability (either accidentally or due to a process failure).
Phishing and other social engineering	Targeted or randomly directed e-mails, or other communications, that successfully gets victims to install malware, remote access, etc., to share their credentials, or otherwise leads to unauthorised entities gaining access.

4.31 For the avoidance of doubt, any cyber-security compromise which results in service disruption of the types set out in Tables 1 and 2 should be reported, regardless of whether or not it aligns to any category in Table 3 (which, as stated, is non-exhaustive).

When to report

4.32 It is important that Providers have adequate processes in place to ensure that reporting is routinely performed and that this reporting continues in all circumstances.

4.33 The Authority expects Providers to make an initial notification in relation to urgent security compromises as soon as possible and usually within 24-hours of the Provider becoming aware of them. The Authority expects this initial notification simply to acknowledge that the Provider is aware of a security compromise, and give an indication of its nature. Any other information that is readily available will be welcomed. Following this initial notification, the Authority then expects the full report to be provided within 72-hours.

4.34 The Authority accepts that, particularly where urgent action is required outside of office hours, this will be a best-efforts activity and not always possible given timing and resource constraints. In the event the Authority has not received a notification from a Provider, and becomes aware of a security compromise appearing to the Authority as requiring urgent action, it will normally seek to make enquiries via the contact point it has been given by the Provider.

4.35 Security compromises should be notified as “urgent” if they meet any of the following criteria:

- Any security compromises impacting service availability, which meet the thresholds set out in Table 1 (fixed network), Table 2 (mobile network) and require urgent remedial action.
- All security compromises involving significant cyber security breaches that are reportable under the "Reportable security compromises” criteria above and which require urgent remedial action.
- Security compromises affecting services to 15,000 or more end users.
- Security compromises affecting services to end users which exceed 5,000 user hours. This should be based on the combination of duration of service loss/disruption and the number of end users affected. Referring to Tables 1 (fixed network) and 2 (mobile network) above, this would be calculated by multiplying columns 2 and 3 in each.
- Security compromises attracting mainstream media coverage, regardless of whether they meet the quantitative thresholds in Tables 1 and 2.
- Security compromises affecting critical Government or local public sector services (e.g. wide spread impact on 999, emergency services communications, etc.).

4.36 Any single security compromise that is likely to affect the provision of wholesale services to both fixed and mobile Providers.

4.37 The Authority expects non-urgent security compromises to be reported within 72 hours of the Provider becoming aware of them. This should include all security compromises affecting services to end users which exceed 2,500 user hours. This should be based on the combination of duration of service loss/disruption and the number of end users affected. Referring to Tables 1 (fixed) and 2 (mobile) above, this would be calculated by multiplying columns 2 and 3 in each.

How to report

4.38 Notification of urgent security compromises should be made using the secure communication method specified by the Authority. This should then be followed by a normal security compromise report using the same secure method.

4.39 All other security compromise reports should be made, whenever possible, within 72 hours of the Provider becoming aware of them and include the information described in the rest of this section and be submitted using the secure communication method specified by the Authority. Where full or final information is not available at the time of reporting, updated reports can be provided as further information becomes available.

4.40 Those Providers notified by the Government of Jersey as needing to demonstrate compliance with the Code requirements should provide the Authority with a contact point for urgent enquiries about significant security compromises. This will allow the Authority to make contact with those Providers where it becomes aware of a significant security compromise which has not yet been reported.

Data required

4.41 Every occurrence of security compromise report sent to the Authority should contain the information below.

1. Provider name

4.42 The full name of the Provider.

2. Provider security compromise reference number

4.43 A unique reference number that can be used to identify the security compromise in communications with the Provider.

3. Date and time of occurrence

4.44 The date and time that the security compromise commenced formatted as: dd/mm/yyyy hh:mm

4. Date and time of resolution

4.45 The date and time that the security compromise was fully resolved, formatted as: dd/mm/yyyy hh:mm. Where the security compromise is ongoing at the time of reporting, the resolution time may be provided when it is available.

5. Location

4.46 The location or locations affected by the security compromise, i.e. Island-wide, parish, district, area, post code, etc. Providers should choose a relevant and understandable description wherever appropriate to explain the geographical area experiencing the service interruption.

4.47 In the case of mobile security compromises resulting in the loss of a technology (e.g. 2G, 3G, 4G or 5G) or service (e.g. voice, data) at specific cell sites, a full list of the affected sites should be provided.

6. Brief description of security compromise

4.48 Provide a short summary of the security compromise, including any relevant information not captured elsewhere in the report.

7. Impact

Services affected

4.49 Provide full details of the services affected. This should identify services as understood by customers, for example telephony, broadband, 2G, 3G, 4G, 5G, etc.

Number/proportion of users affected

4.50 Provide details of the number of users affected by the security compromise. The information provided should be as accurate as is technically feasible at the time of reporting. If a reporting threshold was met under one of the "percentage of users affected" criteria, the Provider should provide the number affected and the percentage of its end users for this service that this represents.

4.51 The Provider should provide details of the total number of affected users against every service associated with a security compromise, even where that service did not meet specific thresholds. For example, for a security compromise which exceeds a voice threshold and also affects data users – but does not exceed a data threshold – the number of data end users affected should be included in the report.

4.52 Where the impact of a security compromise varies over time, effort should be made to explain how this was the case.

4.53 Where exact numbers are not available (for example due to a mobile cell site failure), the Provider should use historical data to estimate the number of end users affected.

4.54 Providers that offer wholesale products to other Providers may have little or no visibility of the number of end users affected by a security compromise within their network or service. The Authority does not expect a Provider to alter their monitoring or reporting systems to obtain this information. However, where it is clear to the Provider that a security compromise is likely

to result in service loss to end users which will exceed the reporting thresholds, they are encouraged to report this.

4.55 A Provider should report qualifying security compromises affecting any service it sells, even if another Provider fulfils the service. However, where a Provider's users use additional services over the top of the network or service it provides, but without its direct involvement, the Authority would not expect the Provider to monitor or report any security compromises affecting such additional services.

Networks and assets affected

4.56 The Provider should provide an overview of the networks and assets affected during the security compromise. At this stage the overview should be brief but the Authority may request further network and asset information during any subsequent investigation.

Fixed and Mobile

4.57 The Provider should indicate if this security compromise has had an impact on both fixed and mobile networks or services.

8. Summary of security compromise cause and action taken so far

4.58 The Provider should explain its understanding of the cause of the security compromise, including its root cause and primary cause when these are known.

4.59 The Provider should provide details of action taken to manage and remedy the security compromise, and any measures taken to mitigate the risk of reoccurrence.

9. Third party details

4.60 If the cause of the security compromise was the failure of a third party service, provide the name of the third party.

4.61 Additionally, indicate whether a service level or operational level agreement is in place with the third party and whether a breach occurred.

10. Name and contact details for follow up

4.62 Details to enable the Authority to follow up on the security compromise if required.

Follow up actions or requirements in response to a security compromise

4.63 Where the Authority believes there are aspects to a security compromise that require further investigation, it will contact the Provider to request further details. This may be through an email, a telephone call or similar, or a follow-up meeting if the Authority believes the security compromise requires a more detailed assessment.

4.64 Within a follow-up meeting, the Authority will examine all aspects of the security compromise, including the Provider's approach to risk management, the cause of the security compromise, its impact and the remedial actions taken. Where a security compromise is technically complex and requires a significant understanding of the Provider's network architecture, topology and design, the Authority may request a presentation of this nature and use its statutory information gathering powers to gather information, if considered appropriate.

4.65 The measures to be taken after the occurrence of a security compromise may include actions or requirements placed on the Provider. For example, where remedying the consequences of a security compromise requires planned changes to the network, the Authority may request regular progress updates.

4.66 In cases where the security compromise is not resolved to the Authority's satisfaction, it may consider the use of assessment and enforcement powers set out in Schedule 2, Part 1 and 2 of the Law.

5 Enforcement

Introduction

5.1 As part of ensuring compliance with the security duties set out under Articles 24K to 24N, 24R and 24TK, the Authority is also responsible for the enforcement of such duties. This section of the Procedural Guidance explains the Authority's approach to enforcement and contains the following content:

- Introduction
- General approach to enforcement
- Power to direct Providers to take interim steps
- Power to impose penalties

5.2 Where the Authority considers enforcement action is needed in association with the telecoms security framework, it will carry this out in a structured way, consistent with the Law and its own evidence-based, proportionate and consistent principles.

5.3 Information which may trigger an enforcement investigation can come to the Authority's attention from a variety of sources, such as a notification by a Provider of a security compromise, through routine compliance monitoring or because of a complaint. Upon triggering the enforcement process, the Authority will complete an initial assessment in order to determine whether to open an investigation. If an investigation is commenced, the Authority will rely upon its statutory powers to obtain the information necessary to take appropriate enforcement action, which may include:

i. requiring information by issuing Security Information Notices;

ii. directing Providers to make a statement specifying whether they are acting in accordance with the provisions of the Code; and

iii. issuing assessment notices.

5.4 Where the Authority determines that there are grounds for action, it will first provide the subject of the investigation with a provisional decision giving them an opportunity to submit representations. Having considered all of the relevant evidence and any representations, the Authority will make a final decision on the case. Where appropriate, the Authority may consider settling a regulatory investigation. Settlement is a voluntary process and leads to a formal, legally binding regulatory decision. Throughout the process, the Authority may rely upon powers introduced by the Law to require Providers to take interim steps or impose a duty to take specified steps by issuing an assessment notice. Under Schedule 2, Part 2, 6 of the Law,

the Authority also has a power to deal with urgent cases, including the power to suspend or restrict a Provider's activity.

The Authority's general approach to enforcement

5.5 In Section 3 above, the Authority provides general guidance about how it envisages exercising its powers to issue Security Information Notices, to issue assessment notices and to direct Telecoms Providers to explain any failure to act in accordance with guidance given by the Minister in the Code. These powers may be relevant also in relation to the Authority's enforcement process.

5.6 As explained above (in paragraph 3.41), the Authority will use these powers where it considers it appropriate, reasonable and proportionate to do so.

5.7 Below the Authority sets out how it generally expects to exercise its power to impose penalties and power to direct a Provider to take interim steps.

Power to direct Providers to take interim steps

Legal framework

Three-stage process

5.8 The Law gives the Authority the power to impose interim steps to a Provider pending the commencement or completion of enforcement action. The process for giving interim directions involves:

- giving a notification setting out the interim steps proposed by the Authority;
- allowing the Provider an opportunity to make representations; and
- issuing a direction to take interim steps.

Notification proposing interim steps

5.9 The Authority may propose interim steps to a Provider only if the conditions set out in Schedule 2, Part 2, 10 (1) of the Law are met. In summary, these conditions are as follows:

- there are reasonable grounds for believing that the Provider has contravened or is contravening a security duty under Articles 25K, 24L, 24M or 24N;
- The Authority either has not yet commenced enforcement action or has commenced but not completed enforcement action;
- there are reasonable grounds for believing either, or both, that a security compromise has occurred or there is an imminent risk of a security compromise, or further security compromise, occurring; and

- it is reasonable to require the Provider to take interim steps given the seriousness or likely seriousness of the security compromise.

5.10 The nature of the "interim steps" which may be required of a Provider is set out in Schedule 2, Part 2, 10(4) of the Law. In summary, these steps include preventing the adverse effects (on the network or service or otherwise) of a security compromise (or a further security compromise), remedying or mitigating the adverse effects on the network or service of a security compromise and eliminating or reducing an imminent risk of a security compromise (or a further security compromise).

Representations

5.11 The Authority may only direct the Provider to take the interim steps once it has been given a notification under Schedule 2, Part 2, 10 of the Law, the Provider has had an opportunity to make representations about the matters notified, the period allowed for representations has expired, and after having considered any representations.

Direction to take interim steps

5.12 The Authority may only direct a Provider to take interim steps if it is satisfied that:

- there are reasonable grounds for believing that a contravention has occurred;
- there are reasonable grounds for believing that a security compromise has occurred as a result of the contravention and/or there is an imminent risk of a security compromise (or a further security compromise) occurring as a result of the contravention; and
- it is reasonable to give the direction, given the seriousness or likely seriousness of the compromise(s) or potential compromise(s).

5.13 A direction to take interim steps must include a statement of reasons and specify the time period within which each interim step must be taken. A direction cannot require a Provider to take interim steps after the completion of enforcement action by the Authority.

5.14 The Authority must commence or complete enforcement action as soon as reasonably practicable after a direction to take interim steps has been given.

5.15 The Authority may, at any time, revoke or vary a direction to make it less onerous.

The Authority's general policy

5.16 As set out above, the Authority can impose interim steps under Schedule 2, Part 2, 10-11 of the Law only where certain conditions have been met.

5.17 As this power is intended to be used in situations where an actual, or potential, security compromise is serious, the Authority expects to be in close dialogue with the Provider to gather

the necessary information to inform its decision on whether directing the Provider to take interim steps would be appropriate under the specific circumstances.

5.18 After receiving a notification setting out the interim steps proposed by the Authority, Providers will have the opportunity to submit their representations, which will be taken into consideration prior to issuing any final directions to take interim steps. Given the urgent nature of a direction to take interim steps, the time given to make representations under Schedule 2, Part 2, 10(2)(c) is likely to be short. The Authority's directions will include a statement of its reasons for issuing the direction as well as the time period(s) for completion of the specified interim steps.

5.19 The Authority may issue such a notification and direction to take interim steps before it has commenced enforcement action, up to any point before it has completed enforcement action. Where the Authority issues such a direction, it must as soon as reasonably practicable commence and complete enforcement action.

Power to impose penalties

Relevant legal framework

5.20 For contravention of a security duty (other than the duty to explain a failure to follow a provision in the Code under Article 24R), the Authority may impose a penalty up to a maximum of ten percent of a Provider's "relevant turnover" or, in the case of a continuing contravention, £10,000 per day.

5.21 For contravention of an information requirement or refusal to explain a failure to follow a provision in the Code (under Article 24R), the Authority may impose a penalty up to a maximum of ten percent of a Provider's "relevant turnover" or, in the case of a continuing contravention, £10,000 per day.

5.22 The Authority must give Providers a period of time to make representations after giving a notification of a penalty before any confirmation decision is made.

The Authority's general policy

5.23 The Authority will consider all the circumstances of the case in the round in order to determine the appropriate and proportionate amount of any penalty.

5.24 The Authority has published penalty guidelines and will have regard to these guidelines in determining the amount of penalty to be imposed under the Law for contravention of a security duty, a failure to comply with an Information Request Notice or a refusal to explain a failure to follow a provision in the Code.

6 Information sharing

Introduction

6.1 The Authority expects to receive information from Providers in connection with the risk and occurrence of security compromises. The Law also provides the Authority with broad information gathering powers that will be used to request information from Providers in connection with the monitoring and enforcement of the telecoms security framework. Information received or collected in these ways will be handled securely and stored appropriately. The Law also permits the Authority to share received or collected information with others in certain circumstances and under certain conditions. This section of the Procedural Guidance explains the Authority's approach to information sharing and contains the following content:

- Introduction
- The relevant legal framework
- The Authority's general policy
- Specific guidance on information sharing

The relevant legal framework

Statutory gateways under the Law

6.2 Under Article 24ZC(2) of the Law, the Authority uses a statutory gateway to disclose information obtained in the exercise of its powers to others providing that, among other things, doing so is relevant and proportionate for the security of Jersey. Others that can receive disclosed information include:

- the Minister;
- a department of the UK Government or government of any other country or territory;
- a Jersey public authority; and
- to another regulator in any country or territory performing a similar function as the Authority.

6.3 The Law also provides statutory gateways for the Authority to share or publish information it has gathered under its telecoms security functions, including:

- under Article 24U(2), the Authority must inform the Minister of the risk or occurrence of serious security compromises;

- under Article 24U(3), the Authority may inform the Minister and others of the risk or occurrence of security compromises; and
- under Article 24Z the Authority must provide a security report to the Minister containing information and advice that may assist in the formulation of telecoms security policy.

6.4 Nothing under Article 24ZC of the Law limits, among others, the disclosure of information under Article 24U, or prevents the publication or disclosure of a report under Article 24Z.

The Authority's general policy

6.5 As part of its telecoms security functions, the Authority plans to share certain information with others involved in telecoms security for the purpose of helping the Authority and others perform their functions. This includes:

- the Minister;
- the DoE, through the Minister, as the Government of Jersey policy lead for the telecoms security sector;
- the JCSC, through the Minister, as lead for promoting and improving Jersey's cyber resilience;[5]
- and other Crown Dependency regulators performing a similar telecoms security function.

There may also be instances in which the Authority would seek to work with the NCSC, as the UK's technical authority for cybersecurity and as part of that, share certain information relating to telecoms security. The Authority expects to disclose such information without prior reference to the Provider, although it will explain the likely extent and basis of such sharing when the Authority requests the information. This will both ensure compliance with legal responsibilities and also benefit Islanders through creating opportunities to enhance telecoms security policy, helping identify new threats and vulnerabilities and remaining abreast of evolving threats and technologies.

6.6 The Authority may also need to share information with other bodies on an occasional basis where appropriate, such as the Jersey Office of the Information Commissioner (**JOIC**), to enable them to perform their respective functions. In this case, the Authority will follow the relevant specific guidance set out below.

6.7 The Authority expects to share both general and specific information on telecoms security with others. General information relates to details about telecoms security that do not relate to any

[5] The JSCS is presently part of the Government of Jersey but expected to become an arm's length organisation created by statute. At this point, it is expected that its governing law will incorporate the statutory gateway allowing the Authority to continue sharing certain information.

specific Provider or Providers, but which may help the Authority and others enhance knowledge, expertise and capabilities relating to telecoms security. Specific information relates to details that may be associated with an individual Provider or Providers. Guidance set out below explains the approach the Authority expects to take for this latter type of information sharing.

Specific guidance on information sharing

Information received through Information Request Notices

6.8 Except for some specific circumstances or unless specifically warranted, the Authority expects to notify Providers at the point of formally requesting information of those parts of the information received that may be shared with others and explain the basis of such disclosure including specifying the relevant statutory gateway being used. Where appropriate, the Authority may ask for a Provider's consent before sharing specific information with others.

Information received through incident reporting

6.9 Providers have a duty under the Law to inform the Authority of any significant risk or occurrence of a security compromise. The Authority has various functions under the Law to inform others in these circumstances.

6.10 Under Article 24U(2), the Authority must inform the Minister in certain circumstances of the risk or occurrence of a security compromise. In this case, the Authority expects to disclose the relevant information without prior reference to the reporting Provider, although the Authority will endeavour to notify them after making the disclosure.

6.11 Under Article 24U(3)(4), the Authority may inform others of the risk or occurrence of a security compromise, including any person who uses or has used the affected network or service, any communications Provider, any person who makes associated facilities available, any overseas regulator, any relevant department of the UK Government and the European Union Agency for Cyber Security. In this case, the Authority will endeavour to inform the Provider before sharing any information, or where this is not possible, the Authority will endeavour to notify the Provider after sharing the information.

6.12 There may also be a need for the Authority to disclose information to third parties for the purposes of exercising their own functions in the interests of the security of Jersey. The Authority expects this will include sharing information with the Minister, as the Government of Jersey's policy lead, the JCSC[6], established by the Minister to be the Government of Jersey's body responsible for promoting and improving the Island's cyber resilience, and other Crown

[6] The Government is establishing the JCSC as an independent legal entity with responsibilities for promoting and improving the Island cyber resilience.

Dependency regulators performing a similar telecoms security function. The Authority expects to disclose such information without prior reference to the Provider, although it will explain the likely extent and basis of such sharing when the Authority requests the information. To the extent that third parties request that the Authority discloses information for the purposes of exercising their own functions, it will endeavour to write to Providers in advance of making such disclosure.

6.13 It may also be necessary for the Authority to disclose information to the Minister to assist in the formulation of policy. In such cases, the Authority will endeavour to write to Providers in advance of making any such disclosures.