Ofcom
making communications work
for everyone

DRAFT REVISED General statement of policy under section 105Y of the Communications Act 2003

Providing procedural guidance on the exercise of Ofcom's functions to ensure compliance with the security duties

Contents

Section

1. Overview

1.1 Under section 105Y of the Communications Act 2003, as amended by the Telecommunications (Security) Act 2021, Ofcom has a duty to publish a statement of their general policy with respect to the exercise of their functions under sections 105I and 105M to 105V of the 2003 Act. This statement, which is made further to that duty and in the exercise of Ofcom's powers under sections 1(3) and 105Y, provides guidance on Ofcom's approach to exercising their functions to seek to ensure compliance with the security duties. In particular, it explains the procedures that we are expecting to follow in carrying out our monitoring and enforcement activity. It also provides guidance about which security compromises we would normally expect providers to report to Ofcom and the process for reporting them.

1.2 In accordance with section 105Y(4), Ofcom will have regard to this statement in exercising our functions under sections 105I and 105M to 105V.

The functions on which we are providing guidance through this statement include:

- Ofcom's power to direct providers to explain any failure to act in accordance with guidance given by the Secretary of State in a code of practice (section 105I);
- Ofcom's general duty to seek to ensure that providers comply with their security duties (section 105M);
- Ofcom's power to carry out, or commission others to carry out, an assessment of whether a provider is complying with the security duties (section 105N);
- Ofcom's power to give assessment notices (section 105O), including issuing an assessment notice which requires a provider to comply with a duty urgently (sections 105P and 105Q);
- Ofcom's duty to publish a statement in our annual report setting out the number of occasions on which premises have been entered pursuant to a duty imposed in an assessment notice (section 105R);
- Ofcom's powers to enforce compliance with the security duties (section 105S), including our power to impose penalties (section 105T) and our power to direct a provider to take interim steps (sections 105U and 105V).

We are also providing guidance about Ofcom's approach to sharing information with other public bodies, including Government, the National Cyber Security Centre and the Information Commissioner.

2. Introduction

The revised security framework

2.1 The Telecommunications (Security) Act 2021 ("the Security Act") amends the security framework in the Communications Act 2003 ("the 2003 Act") with the aim of increasing the security of the UK's public electronic communications networks and services. All providers of public electronic communications networks or public electronic communications services (referred to in this document as "providers") must comply with this revised security framework.

Legislative framework

2.2 The legislative framework includes the following elements, which are discussed in more detail below:

a) The overarching security duties set out in the 2003 Act (sections 105A and 105C);

b) Duties to take specified measures imposed by the Secretary of State by regulations (sections 105B and 105D);

c) Guidance given by the Secretary of State in codes of practice (section 105E); and

d) Duties to report security compromises to Ofcom and to inform users (sections 105J and 105K).

The overarching duties set out in the 2003 Act

2.3 The Security Act amends the 2003 Act, removing existing sections 105A-D and replacing them with strengthened security duties. Section 105A(1) sets out the following overarching duty:

> "The provider of a public electronic communications network or a public electronic communications service must take such measures as 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."

2.4 The term "security compromise" is defined in Section 105A(2) 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 any data stored by electronic means;

(f) anything that occurs in connection with the network or service and causes any 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; or

(g) anything that occurs in connection with the network or service and causes a connected security compromise."[1]

2.5 Further overarching duties are set out in section 105C, which requires providers to take such measures as are appropriate and proportionate to prevent adverse effects arising from a security compromise that has occurred. Where the security compromise has an adverse effect on the network or service, the provider must take such measures as are appropriate and proportionate to remedy or mitigate that effect.

Duties to take specified measures imposed by the Secretary of State by regulations

2.6 The Secretary of State has powers to make regulations under sections 105B and 105D of the 2003 Act which require providers to take certain security measures to meet their security duties set out in sections 105A and 105C of the 2003 Act. In exercise of these powers, the Secretary of State made The Electronic Communications (Security Measures) Regulations 2022 (the "Regulations"), which came into force on 1 October 2022.[2]

[1] Section 105A(3) of the 2003 Act goes on to provide a number of exclusions from this definition.
[2] The Electronic Communications (Security Measures) Regulations 2022 (legislation.gov.uk)

Guidance given by the Secretary of State in codes of practice

2.7 The Secretary of State also has powers to issue codes of practice under section 105E of the 2003 Act giving guidance to providers on the measures to be taken under sections 105A to 105D of the Act. In exercise of these powers, the Secretary of State issued the Security Code of Practice on 1 December 2022, setting out guidance for providers with relevant turnover in the relevant period of more than or equal to £50m (the "Code").[3]

Duties to report security compromises to Ofcom and to inform users

2.8 In addition to the security duties mentioned above, the 2003 Act places certain requirements on providers to report certain security compromises to Ofcom (section 105K) and to inform users about certain risks of security compromise (section 105J).

Ofcom's role in this framework

Monitoring, supervising and enforcing industry compliance

2.9 Ofcom has a general duty under section 105M of the 2003 Act to seek to ensure that providers comply with their security duties. This gives Ofcom a clear remit to work with providers to improve their security and monitor their compliance.

2.10 To allow Ofcom to fulfil this role, the 2003 Act gives Ofcom powers to monitor and enforce industry's compliance with their security duties (sections 105I and 105N to 105V). In particular, it enables Ofcom to require providers to share information that Ofcom considers necessary for the purpose of carrying out its security functions. In addition to exercising its information gathering powers, Ofcom may require a provider to explain their failure to act in accordance with a provision of guidance given by the Secretary of State in a code of practice and issue assessment notices. Assessment notices may include requiring providers to complete system tests, make staff available for interview and permit persons authorised by Ofcom to enter providers' premises to view information, equipment and observe tests.

2.11 Where Ofcom determines that there are reasonable grounds for believing that 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. Ofcom also has a power to direct providers to take interim steps to address security gaps during the enforcement process where certain conditions are satisfied, and Ofcom 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

[3] Electronic Communications (Security Measures) Regulations and Telecommunications Security Code of Practice - GOV.UK (www.gov.uk)

with a notification of contravention, Ofcom can issue financial penalties. These powers are set out in more detail in Section 6.

Reporting functions

2.12 Ofcom also has certain reporting functions under the framework concerning security-related matters. In particular, Ofcom has a duty to inform the Secretary of State about certain risks of security compromise under section 105L, and also must prepare and send to the Secretary of State:

- security reports under section 105Z; and
- infrastructure reports under section 134A.[4]

Duty to inform the Secretary of State

2.13 Section 105L places a duty on Ofcom to inform the Secretary of State about certain risks of security compromise and enables Ofcom to inform the Secretary of State or other persons (either directly or via a provider) about the risk of (or occurrence of) certain security compromises and the technical measures that may be taken in response.

Security reports

2.14 Ofcom is required to provide annual security reports (the first was delivered two years after commencement in 2024, with the second delivered in 2025)[5] to the Secretary of State, containing such information and advice as Ofcom consider may best serve the purpose of assisting the Secretary of State in the formulation of policy in relation to the security of UK public electronic communications networks and services. In particular, such reports must include the following information in respect of the relevant reporting period:

- the extent to which providers have complied with their security duties and acted in accordance with any codes of practice which the Secretary of State may issue, including the Code;
- the security compromises that Ofcom has been informed of;
- the action that Ofcom has taken in response to security compromises that Ofcom has been informed of;
- the extent to which and manner in which Ofcom has exercised its security functions;
- any particular risks to the security of public electronic communications networks and service that it has become aware of; and
- any other information of a kind specified in a direction given by the Secretary of State.

2.15 The Government can publish these reports or extracts from them.[5]

Infrastructure reports

[4] See, in particular, section 134B(1)(ha) and section 134B(2)(fa). In addition, Ofcom may prepare and publish additional reports under section 134AA of the 2003 Act.
[5] Section 105Z(6)-(8) of the 2003 Act.

2.16 The 2003 Act also imposes duties on Ofcom regarding what is to be included in its infrastructure reports under Section 134A of the 2003 Act (currently called 'Connected Nations'). We produce these reports annually and are required to send them to the Secretary of State and publish them, which we do on our website[6].

2.17 In addition to the other matters listed in section 134B, Ofcom's infrastructure reports must deal with the extent to which providers of public UK networks and services are complying with their security duties under sections 105A to 105D of the 2003 Act.

Working with other public bodies

2.18 The Department for Science, Innovation and Technology (DSIT) is the Government policy lead for the telecoms security sector, and the National Cyber Security Centre (the "NCSC") is the UK's technical authority for cybersecurity. Ofcom works with both organisations, using information sharing gateways so that information can be shared where necessary. Further detail on information sharing is set out in section 7.

What this guidance covers

2.19 This document provides general guidance about Ofcom's approach to exercising our functions in relation to:

- supervisory compliance monitoring (section 3);
- testing (section 4);
- reporting security compromises, both to Ofcom and to users (section 5) [7]
- enforcement (section 6);
- and about Ofcom's approach to sharing information with other relevant public bodies (section 7).

[6] Connected Nations and infrastructure reports - Ofcom
[7] Link to 72-hour reporting template on Ofcom website

3. Supervisory compliance monitoring

Introduction

3.1 As explained above, under section 105M of the 2003 Act Ofcom has a general duty to seek to ensure that providers comply with their security duties imposed on them by sections 105A to 105D, 105J and 105K.

3.2 In this section, we set out our approach to monitoring compliance with these security duties. Specifically, we describe our supervisory model, setting out the principles behind our approach, explain our process for identifying into which "tier" (as described in the Code) each provider falls, before going on to provide guidance on our enforcement functions under sections 105I and 105N to 105V to monitor and enforce industry's compliance with the security duties, including how we expect to use our powers.

Principles behind Ofcom's approach to compliance monitoring

A supervisory model

3.3 The Security Act introduced significant changes to the regulation of security in the communications sector. This is true not only in relation to the greatly expanded range of security duties on providers but also in relation to Ofcom's role and the powers available to us for monitoring and seeking to ensure, and enforcing, compliance.

3.4 We expect providers to ensure that they understand and comply with the relevant obligations in the 2003 Act (as amended by the Security Act) and any associated regulations. They should also be aware of the guidance on measures to be taken under the 2003 Act contained in any codes of practice issued by the Secretary of State.

3.5 The threats faced by providers continue to evolve, requiring a strong security risk management culture to meet Government's aim of improving the security of the telecommunications sector through use of the security framework introduced by the Security Act. The key objective of our role since commencement has therefore been to determine if each provider is implementing appropriate organisational and technical measures at sufficient pace as they continue to work towards full compliance.

3.6 Our intention is to build our understanding of the security measures that providers are taking through our supervisory programme which will assess whether providers are complying or have complied with their security duties using a mix of our powers. As explained further below in 3.16, we will continue to use our information gathering programme to assess progress against the Code, alongside targeted supervision of specific providers or security themes, and the use of other relevant powers where necessary. We stand ready to exercise our full suite of enforcement powers where providers do not meet their obligations. Our approach to enforcement is set out in Section 6.

Supervision based on tiering

3.7 Although aspects of the framework, such as the overarching duties in the 2003 Act, apply to all providers, what is appropriate and proportionate in any particular case is likely to differ depending on the size of the provider. The Code reflects this by adopting the following three-tier approach:

- Tier 1 (relevant turnover of > £1bn): The largest national-scale providers, whose availability and security is critical to people and businesses across the UK.
- Tier 2 (relevant turnover of £50m-£1bn): Medium sized providers. The Code indicates that these providers will have more time than Tier 1s to implement some of the measures it contains.
- Tier 3 (relevant turnover below £50m, but who are not micro-entities): Although the overarching duties in the Act apply to all smaller providers, micro-entities are exempt from the Regulations[8] and the Code does not apply to any Tier 3 providers. For further details on the Government's tiering system, see the Code (paragraphs 0.11-0.16) and the Government response (Part 2).

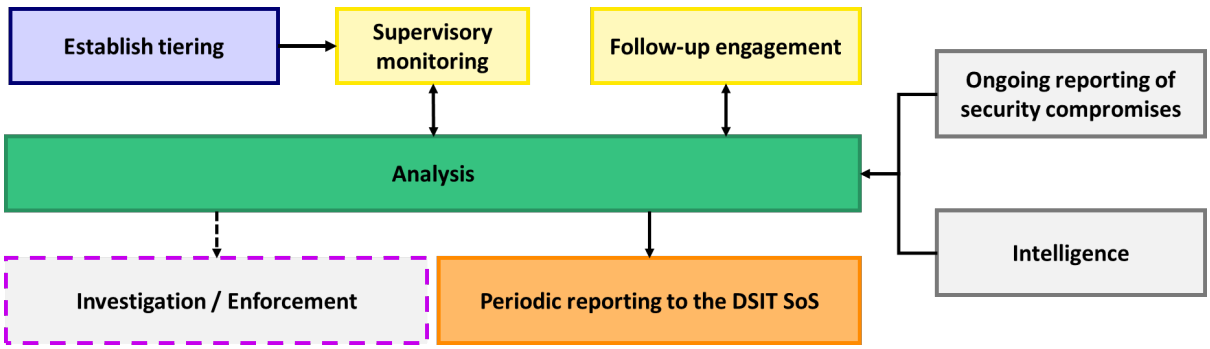
Our approach to supervising Tier 1 and Tier 2 providers

3.8 Our activities focus on providers in Tiers 1 and 2. This is consistent with the approach taken in the Code, balancing the need for security with the size and criticality of the networks and services involved. The rest of this section explains our approach to this supervision.

3.9 Providers' implementation of measures has evolved over time and will continue to do so as they work towards the phased timelines in the Code. Since commencement, our work has significantly improved our understanding of provider networks, services and compliance approaches and this understanding will continue to develop as implementation advances. Our supervisory approach is depicted in Figure 1.

[8] Regulation 16 of the Regulations contains an exemption for cases where the network provider or service provider is a "micro-entity" as defined by that regulation.

Figure 1- Ongoing supervisory approach for Tiers 1 and 2



Establishing tiering

3.10 Ofcom uses the thresholds in the Code to determine which tier providers are in. The information required for this forms part of our general demand[9] for data on relevant turnover, which is used for tiering alongside other purposes such as setting our annual administrative charges.

3.11 We inform providers whose relevant turnover means they will be subject to our supervision, as well as any that move between tiers, in accordance with the guidance in the Code.

3.12 We do not inform providers falling into Tier 3 or micro-entities, so any providers who do not hear from us can assume they are not part of the Tier 1 and Tier 2 supervision approach set out in this guidance. Tier 3 providers are still required to comply with their legal obligations, and Ofcom could use its powers to investigate potential breaches and take enforcement action where necessary. Moreover, where we identify a Tier 3 provider as delivering a key service, or one of increasing significance, we may also supervise such services if we identify the specific services provided as being of particular significance.

Information-gathering powers (section 135)

Legal framework

3.13 Ofcom has broad information gathering powers under section 135 of the 2003 Act which enable us to gather any information we consider necessary for the purpose of carrying out our functions under the 2003 Act, including:

a) for the purpose of carrying out an assessment under section 105N of whether a provider is complying or has complied with its security duties under sections 105A to 105D, 105J and 105K (section 135(3)(iza));

[9] See Ofcom's General demand for information

b) for the purpose of preparing a report under section 105Z of the Act (i.e., a security report to the Secretary of State; section 135(3)(izb));

c) for the purpose of assessing the risk of a security compromise occurring in relation to a public electronic communications network or service (section 135(3)(izc));

d) to facilitate the provision of "security information" (section 135(3C)) by requiring a provider:

i) to produce, generate or obtain security information;

ii) to collect or retain security 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 security information.

3.14 The information that Ofcom can require from a person can include information concerning future developments of a public electronic communications network or services that could have an impact on the security of the network or service (section 135(3A)(za)).

Ofcom's general policy

3.15 We are required to take into account relevant provisions in any code of practice when assessing compliance[10], so, in 2022, we put in place a rolling programme of information notices issued under section 135 of the 2003 Act ("section 135 information notices") to gain an understanding of each provider's compliance with their security duties and adherence to any codes of practice, including the Code, and any alternative or additional compliance measures a provider was taking. The Code itself sets out a series of dates spanning from 2024 to 2028, reflecting Government's expected timescales for implementing the different measures. We have therefore been broadly aligning the order in which we requested information about measures with the relevant dates set out in the Code.

3.16 We will continue to use information notices. However, as our understanding of compliance matures, we will evolve our approach to focus on specific security themes of concern, using other powers where appropriate to better understand providers' compliance with their security duties and adherence to any codes of practice.

3.17 In most cases, we will send drafts of our section 135 information notices to providers for comment before finalising them. In particular, we would normally expect to do this when we are gathering information as part of our ongoing programme. This is in line with our general policy on information gathering.[11]

3.18 Where we use information notices, we will often issue these directly to the relevant providers of PECN/PECS. However, we may also gather information from other relevant

[10] Communications Act 2003 - Section 105H(3)
[11] See Ofcom's policy statement on information gathering.

persons (section 135(2)), such as persons making associated facilities available to the relevant providers, where we consider it necessary to carry out our functions.

3.19 In addition to issuing section 135 information notices as part of our regular monitoring activity, it may also be appropriate to use other powers to gather information that will inform our supervision and enforcement activity. As mentioned above, these powers include, in particular, Ofcom's powers to direct providers to explain any failure to act in accordance with guidance given by the Secretary of State in a code of practice and Ofcom's powers to give assessment notices (which are discussed below).

3.20 The information that we gather from providers is also used to assist us in preparing our security report and infrastructure report to the Secretary of State.

Information-gathering programme

3.21 To date, we have issued an initial section 135 information notice covering network and service assets in scope, alongside some Code measures, then a further three section 135 information notices at no less than nine-month intervals, each allowing providers a six-month response period. Where we use information notices in future, we expect the cadence to be one every twelve months rather than nine.

3.22 This approach may also need to be amended 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

3.23 We may need to improve our understanding of a provider's compliance, seek clarification, or additional information beyond that included in a provider's written response to a section 135 information notice. Where appropriate, we would expect to do this via correspondence and meetings. We will give reasonable notice of any such meetings and limit them to those that we consider necessary in order to develop a sufficiently thorough understanding of the measures taken by providers to comply with their security duties.

Handling sensitive data

3.24 We use an appropriate platform to securely process and store confidential information received from providers as part of the regime. This enables us to manage, store and review information sent to us via a secure gateway.

3.25 Operational arrangements for providers to send us sensitive data in a suitable secure manner will be clarified as and when we issue such requests.

Information sharing

3.26 In Section 7, we provide general guidance about Ofcom's approach to sharing information with other public bodies, including Government, the National Cyber Security Centre and the Information Commissioner.

Power to direct providers to explain any failure to act in accordance with a code of practice (section 105I)

Legal framework

3.27 A failure to act in accordance with a provision of a code of practice(s) issued by the Secretary of State does not of itself make a provider liable to legal proceedings (section 105H(1)). However, Ofcom may notify a provider where we have reasonable grounds for suspecting that the provider is failing or has failed to act in accordance with a code provision (section 105I(1)). The notification must:

- set out (i) the relevant provision(s) of the code of practice 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 (section 105I(2)).

3.28 In its statement, the provider must confirm whether or not it is failing, or has failed, to act in accordance with the provision of the code of practice and explain the reasons for its response (section 105I(3)-(4)).

Ofcom's general policy

3.29 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, we expect providers to take proactive steps to meet their regulatory obligations.

3.30 It is our intention to use a variety of powers to assess whether providers are complying with their security duties, taking into account any relevant provisions set out in any codes of practice, including the Code. Where information we gather gives us reasonable grounds to suspect providers are not acting in accordance with any such code, we may use our section 105I powers. We will use any information provided to inform our compliance assessments and when considering any subsequent enforcement action.

3.31 In practice, we expect providers to engage constructively with our monitoring processes and provide a clear picture of the steps they are taking towards compliance when providing information in response to our section 135 information notices. Therefore, we only anticipate using our section 105I power where we consider that a clear statement from a provider of the type required under section 105I is necessary for us to consider whether further escalation might be appropriate. Any use of this power will take into

account the implementation timelines attached to provisions in any codes of practice, including the Code.

Powers to assess compliance – Assessments and assessment notices (sections 105N-105Q)

Legal framework

Duties specified in Ofcom's assessment notices

3.32 Sections 105N to 105R of the 2003 Act set out Ofcom's powers to assess providers' compliance with their security duties.

3.33 Section 105N gives Ofcom 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 sections 105A to 105D, 105J and 105K. Providers have a duty to cooperate with an assessment. Providers are also required to pay Ofcom's reasonably incurred costs in connection with the assessment.

3.34 Section 105O provides Ofcom with the power to give providers an assessment notice for the purpose of carrying out an assessment under section 105N. It sets out what an assessment notice may require a provider to do. Specifically, it may require a provider to:

- carry out specified tests (or tests of a specified description) in relation to the network or service (section 105O(2)(a));
- make arrangements for another person to carry out specified tests (or tests of a specified description) in relation to the network or service (section 105O(2)(b));
- make people available for interview (section 105O(2)(c)). These must be people 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 (section 105O(2)(d)-(k)) (this power of entry is discussed in more detail in the "Power to enter premises" section below).

3.35 Such notices cannot require a provider to do anything before the end of the period within which the notice can be appealed under section 192 of the 2003 Act.

3.36 Section 105P allows Ofcom 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. Section 105Q 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.

Ofcom's general policy

3.37 We may consider issuing assessment notices under section 105O or section 105P to understand the security measures that providers are taking when it is appropriate and proportionate to our assessment of whether a provider is complying or has complied with its security duties. This includes, where appropriate, using assessment notices to inform our enforcement activity. The use of such notices would not necessarily indicate an escalation in our compliance concerns, but may offer a more proportionate way of ascertaining the information we need than reliance on section 135 information notices in some cases.

3.38 Our assessment 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.

3.39 Where it is appropriate to do so, we will send draft assessment notices to providers for comment before finalising them.

3.40 We note that providers have a duty to cooperate with an assessment under section 105N. In our view, 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. Ofcom has powers to enforce any breach of this duty of co-operation (section 105S).

Powers to assess compliance – Power to enter premises (section 105O and 105R)

Legal framework

Duties specified in Ofcom's assessment notices

3.41 As part of Ofcom's powers to assess providers' compliance with their security duties under sections 105N to 105R, section 105O permits Ofcom to issue assessment notices that require providers to do various things, which include permitting an Ofcom employee or other person authorised by Ofcom (an "authorised persons")[12] to enter non-domestic premises[13] for various purposes. Specifically:

- to observe any relevant operations taking place (105O(2)(e));
- to direct an authorised person to relevant equipment or other material (105O(2)(f)) or documents (105O(2)(g)) 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 (105O(2)(h));

[12] Section 105O(12).
[13] Section 105O(2)(d) and 105O(5).

- 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 (105O(2)(i));
- 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 (105O(2)(j));
- to provide an authorised person with an explanation of such documents, information, equipment or material (105O(2)(k)).

Referring to Ofcom's exercise of our power of entry in our annual reports

3.42 Section 105R requires Ofcom to publish a statement which sets out the number of occasions on which premises have been entered pursuant to the duty imposed under section 105O(2)(d) in its annual report.

Ofcom's general policy

3.43 In exercising our powers of entry, we expect to have regard to the Home Office's code of practice on powers of entry, where relevant.

3.44 We will set out the number of times premises have been entered during the course of each financial year in our annual report. Ofcom's previous annual reports can be found on our website[14].

[14] https://www.ofcom.org.uk/about-ofcom/annual-reports-and-plans

4. Testing

Introduction

4.1 Testing covers a wide variety of different techniques and scenarios, which are used at different times for different reasons. This section explains how Ofcom expects to use its expanded powers under section 105N of the 2003 Act to monitor compliance with the security duties. We also explain the continuing role for the voluntary penetration testing framework (known as "TBEST") which we will continue to run in parallel.

Legal framework

4.2 As explained above, section 105N of the 2003 Act gives Ofcom 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 sections 105A to 105D, 105J and 105K. Section 105O provides Ofcom with the power to give providers an assessment notice for the purpose of carrying out an assessment under section 105N. See above for further details on Ofcom's powers relating to assessments under sections 105N to 105R.

4.3 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 (section 105O(2)(a));
- make arrangements for another person to carry out specified tests (or tests of a specified description) in relation to the network or service (section 105O(2)(b)).

4.4 A test required by an assessment notice may include tests which risk causing a security compromise, 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 (section 105O(4)).

Testing required under this framework

4.5 Regulation 14 requires providers to carry out periodic testing as is appropriate and proportionate to identify the risk of security compromises occurring. We expect providers to conduct a variety of testing practices to identify risks of security compromises for the purposes of remediation and anticipate that our supervision will at times focus on this area. Guidance on testing can be found in section 13 of the Code.[15]

4.6 We may also decide that it is appropriate to mandate testing under section 105O for the purposes of an assessment under section 105N.

[15] Telecommunications Security Code of Practice

Voluntary testing

4.7 Ofcom operates a voluntary, collaborative testing programme called TBEST. Regular voluntary TBEST participation may reduce the likelihood that testing will be required under section 105O for the purposes of an assessment under section 105N, as it provides assurance on the effectiveness of a provider's overall security controls. Providers can learn more about this programme in the TBEST handbook, accessible on the Ofcom website.[16]

[16] TBEST handbook

5. Reporting security compromises

Introduction

5.1 Sections 105J and 105K place duties on providers to tell users about the risk of a security compromise, and to tell Ofcom about security compromises, respectively. This section outlines our expectations in relation to these duties.

5.2 We note that the definition of security compromise under section 105A(2)-(3) of the Act covers resilience-related incidents as well as cyber attacks.

Duty under section 105J to inform users of risk of security compromise

Legal framework

5.3 Where there is a significant risk of a security compromise occurring in relation to a public electronic communications network or a public electronic communications service (section 105J(1)), the relevant providers must take such steps as are reasonable and proportionate to inform those users who may be adversely affected by the security compromise about (section 105J(2)-(3)):

- 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.

Ofcom's general policy

5.4 The duty to inform users of the risk of a security compromise applies where there is both a "significant risk of a security compromise occurring" and 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, we would not expect users to be informed of such matters under section 105J.

5.5 There are a number of factors which should be considered when determining whether users should be informed about a given risk of a security compromise. These include:

- Does the risk arise from a vulnerability for which there is a known 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 that are likely to able to exploit any related vulnerability and likely to do so in a way which adversely affects users of the network or service?

5.6 If it is determined that there is indeed a significant risk of a security compromise occurring, and that users may be adversely affected by this, providers must take steps to inform relevant users. What will be required by section 105J 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. There are two broad categories as to the approach that might be adopted:

- **Direct contact.** This is contact that may be personalised for user or location of user, i.e., addressed to a specific named user or location, and could be sent via email, push notifications, 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 or impersonalised contact, i.e., not addressed to a named user or location, through email or push notifications.

5.7 Factors which we consider 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.

5.8 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 direct contact approach.

5.9 After providers become aware of the risk of a security compromise, they must also consider at what point in time relevant information should be shared with users. We would expect that providers will ensure they have a high degree of confidence that the information they are going to share is accurate before doing so. However, in situations where rapid action could be taken by an informed user in order to reduce their exposure to harm, we would expect that sufficient information to enable this would be shared as quickly as reasonably practicable.

Security compromise reporting to Ofcom under section 105K

Legal framework

5.10 Section 105K(1) requires providers to inform Ofcom 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.

5.11 Section 105K(2) 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;
>
> (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."

Ofcom's general policy

5.12 Security compromises required to be reported to Ofcom under section 105K include "anything that compromises the availability, performance or functionality of the network or service" (section 105A(2)(a)). We expect the majority of these sorts of network or service outages, often known as 'availability' or 'resilience' incidents, to be reported to Ofcom under this requirement.

5.13 The definition of security compromise in section 105A(2) 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 section 105(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 section 105K 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 4 below.

5.14 We note in particular that section 105K(1)(b) states that the following is also reportable:

> "any security compromise within section 105A(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".

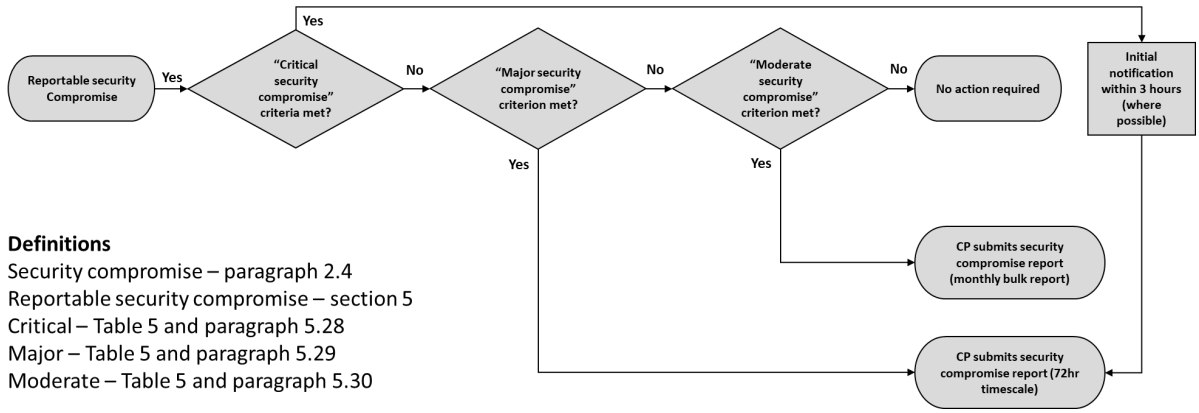
5.15 Therefore, any event that puts any person in a position, however briefly, to be able to bring about a further security compromise that would have a significant effect, must also be reported (*even where the provider's existing defences make a successful follow-on attack unlikely, and even where multiple layers of defence remain between the attacker's initial access and the point at which significant harm could be caused*). These types of compromises are commonly referred to as "pre-positioning attacks". 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.[17]

5.16 The remainder of this section sets out further guidance for industry on:

- **Which security compromise 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
- **How to report**, including information on contact information and guidance on our reporting template for security compromises

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

Figure 2: Process for reporting security compromises



Which security compromises to report

5.18 The criteria and thresholds set out below, based on the factors listed in section 105K(2), set out our view of which security compromises are likely to be significant and should therefore be reported to Ofcom. If any one of the criteria or thresholds is met, the provider

[17] As was seen in the case of initial exploitation by Salt Typhoon: Salt Typhoon is nomenclature given by Microsoft Threat Intelligence for a Chinese nation state-aligned threat actor that has been known to target the telecommunications industry.

should submit a security compromise report. Ofcom has the power to take enforcement action where providers do not report in accordance with the statutory requirements. If an incident has a significant effect on the operation of the network or service but does not meet the threshold, it is still reportable to Ofcom by virtue of the duty under section 105K.

5.19 Reportable security compromises under our criteria and thresholds are as follows:

- Any security compromises impacting service availability, which meet the thresholds set out in Table 1,Table 2 or Table 3 below[18];
- 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;
- Security compromises affecting critical Government or public sector services (e.g. widespread impact on 999, 3-digit non-emergency numbers, emergency services communications);
- Any security compromises that the provider is aware of that has a link to a potential loss of life;
- Any security compromises involving significant cyber security breaches (see illustrative examples in Table 4);
- Any security compromises reported to other Government agencies or departments;
- Any security compromises that providers are aware of being reported in the media (local, national or trade news sources);
- Any single security compromise that is likely to affect the provision of wholesale services to both fixed and mobile providers in a given geographical area.

Table 1- Fixed network numerical thresholds

Network/service type	Number of end customers affected	Duration of service loss or major disruption
Fixed network providing access to the emergency services	≥1,000	≥1 hour
Fixed network providing access to the emergency services	≥100,000	Any duration
Fixed voice or data service/network offered to retail customers	≥10,000 or ≥25%[2]	≥8 hours

[18] For repeat security compromises, the provider should combine the impacts of the individual security compromises in determining whether they meet the numerical thresholds. Repeat security compromises are considered to be those which reoccur within four weeks or are separate security compromises affecting the same services in the same areas over a four-week period.

Fixed voice or data service/network offered to retail customers	≥100,000	≥1 hour

Notes on Table 1:

1. *A customer 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 10,000 end customers or 25% of the provider's total number of end customers on the affected service, whichever is the lowest number*

Table 2- Mobile network numerical thresholds

Provider type	Number of end customers/cell sites affected [1]	Duration of service loss or major disruption
Mobile network operators (MNO) and mobile virtual network operators (MVNO)	≥10,000 customers [2] or ≥25% of customer base [5]	≥8 hours
	≥100,000 customers	Any duration
MNO	≥25 cell sites [3]	≥2 hours
	≥150 cell sites	Any duration
	≥1 rural [4] cell site	≥8 hours

Notes on Table 2:

1. *We expect MNOs to include the number of customers affected as part of their incident report as well as the number of cell sites where applicable.*
2. *A customer is affected if the main functions of a network or service are not available to them due to the security compromise.*
3. *A cell site is affected if the main functions of a network or service are not available to customers due to the security compromise.*
4. *A rural cell site is affected where the postcode of the physical location of the impacted cell site matches a postcode in our rural dataset.*
5. *This threshold should be interpreted as 25% of the provider's total number of end customers on the service affected.*

Table 3- Broadcast network numerical thresholds

Network/service type	Number of end customers affected[1]	Duration of service loss or major disruption
Broadcasting service/network for reception by the general public	≥100,000	≥12 hours

Notes on Table 3:

1. A customer is affected if the main functions of a network or service are not available to them due to the incident.

5.20 Where a provider expects emergency roaming would have allowed customers in the affected area to retain 112/999 access, such an incident remains a reportable security compromise.

5.21 Where providers operate a PECN/PECS, they are required to report security compromises that meet the criteria set out in Tables 1, 2 and 3. This applies equally in the case where the impact on their customers is due to an issue on a third party's network or service. If providers are reliant on a third party (such as an MNO), we expect them to collect the required information and include this in any report. Providers cannot rely on their third party to report on their behalf. This applies also to providers that offer wholesale products to other providers, who may have little or no visibility of the number of end customers potentially affected. We do 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 customers which will exceed the reporting thresholds, we would expect wholesale providers to report this. We recognise that this could result in duplicate reporting.

5.22 Providers should report if any combined interruptions in their service reach the thresholds. This could be in instances of severe weather (for example, storms, heatwaves, space weather) and does not need to be localised.

5.23 For illustrative purposes, Table 4 below sets out a non-exhaustive list of examples of cyber-security compromises which we expect to be reportable. We will keep this list under review and update it as necessary if we become aware of other categories of cyber-security compromise which we consider are likely to be reportable.

5.24 For the avoidance of doubt, any cyber-security compromise which results in service disruption (or puts the attacker into a pre-position scenario) of the types set out in Tables 1, 2 and 3 should be reported, regardless of whether or not it aligns to any category in Table 4 (which, as stated, is non-exhaustive).

Table 4- Examples of reportable cyber-security compromises

Category	Explanation
Supply chain compromise[19]	Products used in a provider's network/service are compromised, as a result of an attack on the supplier
Successful Exploitation of Vulnerability[20]	An external attacker carrying out a targeted internet-based attack

[19] SolarWinds, Syniverse
[20] Compromise of TalkTalk internet Facing Website

Physical attacks[21]	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[22]	An external attack via a Managed Service Providers (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[23]	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[24]	Either a targeted or "random" attack that encrypts data for ransom and/or extracts data for ransom
Internet routing protocol abuse[25]	When attackers reroute internet traffic (maliciously, or due to misconfiguration). Examples include BGP hijacking and DNS poisoning.
Security misconfiguration[26]	Systems are not correctly/insufficiently secured leaving an exploitable loophole/vulnerability (either accidentally or due to process failure)
Phishing and other social engineering[27]	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 un-authorised entities gaining access.

When to report

5.25 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.

Table 5 - Quantitative reporting severities

Severities	Impact on users	Impact on cell sites
Critical (3hr notification + 72hr report)	≥1,500,000 user-hours lost OR ≥10,000,000 end users.	≥150 sites
Major (72hr report)	≥250,000 user-hours lost	

[21] Mobile masts attack during COVID
[22] Global targeting enterprises managed service providers
[23] Former Ubiquiti employee charged with hacking, extorting company
[24] Wannacry (NHS, Telefonica Spain etc), NotPetya (Maersk)
[25] BGP hijacking
[26] T-Mobile data breach
[27] Phishing guidance

Moderate (monthly bulk report)	≤ 250,000 user-hours lost	≥25 sites OR ≥1 rural site(s)

5.26 We expect providers to make an initial notification to Ofcom in relation to a critical security compromise as soon as possible, and usually within 3 hours of the provider becoming aware of them. We expect this initial notification simply to acknowledge that the provider is aware of such security compromise, and give an indication of its nature. Any other information that is readily available will be welcomed. We then expect the completed reporting template to be provided within 72 hours. [28] Providers should bear in mind that Ofcom may require further information about a security compromise after a report has been provided.

5.27 We accept 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 that we have not received a notification from a provider, and become aware of a security compromise appearing to us to require urgent action, we will normally seek to make enquiries via the contact point we have been given by the provider.

5.28 Security compromises should be notified as "critical" if they meet any of the following criteria:

- 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 attracting local, national or trade media coverage, regardless of whether they meet the quantitative thresholds in Tables 1, 2 and 3.
- Security compromises affecting services to 10 million or more end users.
- Security compromises affecting services to end users which exceed 1.5 million user-hours. This should be calculated by multiplying the number of end customers affected by the duration of the service loss/disruption.
- Security compromises attracting national mainstream media coverage, regardless of whether they meet the quantitative thresholds in Tables 1, 2 and 3
- Security compromises affecting critical Government or Public Sector services (e.g. wide spread impact on 999, 3-digit non-emergency numbers, emergency services communications).
- Any security compromises that the provider is aware of that has a link to a potential loss of life.
- Any single security compromise that is likely to affect the provision of wholesale services to both fixed and mobile providers in a given geographical area.

5.29 We expect major security compromises to be reported within 72 hours of the provider becoming aware of them. This includes any reportable security compromises as listed under reportable security compromises (5.19) that are not classed as critical (5.28).

[28] 72-hour reporting template

5.30 Moderate security compromises may be excluded from the 72-hour reporting requirement above and instead included in monthly bulk reporting.

5.31 Providers should report to Ofcom all bulk security compromises which commenced in a calendar month before the second Monday of the following month.

5.32 The template for bulk reporting can be found here.

5.33 To facilitate Ofcom's annual reporting, providers should keep data for security compromises that have been reported for no less than 13 months following security compromise resolution.

How to report

5.34 Notification of critical security compromises should be made directly to the 24-hour security compromise reporting number: 0207 981 3184. This should then be followed by a normal security compromise report. All security compromise reports should be submitted to incident@ofcom.org.uk.

5.35 All major security compromise reports should be made within 72 hours of the provider becoming aware of them, include the information described in the rest of this section, and be submitted using the template. Where full or final information is not available at the time of reporting, updated reports should be provided as further information becomes available.

5.36 If providers require a secure environment for submitting a security compromise report then a request should be made to the email address above and additional guidance will be provided.

5.37 Those providers notified by Ofcom as falling within Tier 1 and Tier 2 should provide Ofcom with a contact point for urgent enquiries about significant security compromises. This will allow Ofcom to make contact with those providers where we become aware of a significant security compromise which has not yet been reported.

Data required

1. Provider name

5.38 The full name of the provider.

2. Provider security compromise reference number

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

3. Date and time of occurrence

5.40 When the security compromise occurred or was first discovered. 24-hour format is expected as: DD/MM/YYYY HH:MM.

4. Date and time of resolution

5.41 The date and time that the security compromise was resolved. 24-hour format is expected 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. Current incident status

5.42 Whether the security compromise is ongoing or resolved.

6. Security compromise overview

5.43 Details of the security compromise being reported. Where known, details should include:

- How was the security compromise first detected/discovered? e.g. drop in data traffic, increase in customer complaints, alerts from monitoring/NOC etc.
- High-level timeline of events up to the point of report.
- If the security compromise was cyber-related, whether this was under section 105K (1)(a) and/or section 105K(1)(b).
- Root cause (if known):
  - For cyber-type security compromises (e.g. supply chain compromise, exploitation of vulnerability, physical attack, managed service-based attack, insider attack, ransomware attack, internet routing protocol abuse, security misconfiguration, social engineering etc.).
  - For resilience-type security compromises (e.g. human error, severe weather, change related, power failure, cable faults, hardware faults, software faults, misconfiguration etc.).
- Actions taken to manage, contain, isolate, or resolve the security compromise.
- If applicable, details of third-party causation. This should include the name of the third party, whether a service level or operational level agreement is in place with them and whether the security compromise affected them also.
- Glossary of all terminology/nomenclature used in the submitted report.

7. Affected services and assets

5.44 Full details of the services affected. This should identify services as understood by the customer and could include, without being limited to:

- Broadband – FTTP, FTTC
- VOIP/digital voice
- PSTN
- Mobile – if known affected technologies e.g. 2G-5G
- Satellite

5.45 The provider should provide an overview of the networks and assets that were affected during the security compromise. Affected assets could include, without being limited to:

- Access
- Backhaul
- Core

5.46 If we decide to investigate the security compromise further, network and asset information may be required to a level of detail commensurate with the following:

- ENISA Technical Guideline on Threats and Assets (Section 5) for legacy networks & services, and virtual/5G networks & services.

5.47 Where possible, please inform us whether any assets affected were Network Oversight Functions (NOFs) and/or Security Critical Functions (SCFs).

8. If applicable, effect on access to emergency services

5.48 This includes the ability to share location information. The ability for mobile phones to roam onto available networks to make an emergency call (i.e., not dependent on their home network) should not negate the need to account for the potential impact.

9. Number/percentage of affected voice users (fixed line & mobile)

5.49 If a reporting threshold was met under one of the 'percentage of users affected' criteria, the provider should provide the number of users affected and the percentage of the provider's end customers that this represents.

5.50 The provider should give details of the total number of affected customers for every service associated with a security compromise including voice and data.

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

5.52 Where exact numbers are not available (for example, due to a mobile cell site failure), we expect the provider to use historical data to make a reasonable estimate of the number of end customers affected. Providers should take into consideration any substantial, well-publicised changes in user density due to festivals, sporting events or similar.

5.53 Providers which offer wholesale products to other providers may have little or no visibility of the number of end customers affected by a security compromise with their network or service. We do 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 customers which will exceed the reporting thresholds, we would expect them to report this. We recognise this could result in duplicate reporting.

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

10. Number/percentage of affected data users (fixed line and mobile)

5.55 See guidance from <5.49 to 5.54>.

11. Location

5.56 Location information should describe the geographical location of the impact of the security compromise. Where possible, a UK postcode should be provided which identifies the geographical area where service interruption was experienced.

5.57 Where the geographical impact of a security compromise is not easily attributable to a single or small number of complete postcodes, the provider should provide a single or series of summary postcodes which will contain only the 'outward' part of the postcode.

5.58 Where an issue has regional or national impact, the provider should provide the name of the region or nation in lieu of a postcode.

5.59 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, with global cell IDs.

5.60 Use the following examples as a guide:

Table 5 - Providing location information

Failure location examples	**Location expectation**
Service interruption due to RAN failure at a single or number of cell sites	The global cell ID(s)
Service interruption due to failure at a single or small number of street cabinets	The full post code of the street cabinet(s)
Service interruption due to issues associated with a single or a small number of exchanges	The full post code of the exchange(s)
Service interruption to the whole of Leeds city centre	The 'outward' part of the Leeds city centre post code. In this example 'LSECTION 1' would be appropriate.
Service interruption with impact across the whole of Manchester	In this case the provider should report the location as 'Manchester'.
Service interruption with impact across an entire county/region	In this case the provider should report the name of the county/region.
Service interruption with national impact	'UK', 'England', 'Scotland', 'Wales', 'Northern Ireland', with 'north', 'south, 'east' and 'west' designations as appropriate. E.g. Northwest England.

5.61 To enable Ofcom to accurately map incidents using global cell IDs, mobile network providers should provide us with information about their RAN on a monthly basis in the format of the Ofcom cell data standard.[29]

Follow up actions or requirements in response to a security compromise

5.62 Where it is felt that there are aspects to a security compromise that require further investigation, we will contact the provider to request further details.

5.63 If we require clarification of data provided in the report submitted by a provider, contact will be made by email or telephone. If we believe that a detailed investigation of the security compromise is required, we will typically invite the provider to a follow-up meeting.

5.64 Ofcom will use the follow-up meeting to 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, Ofcom may request a presentation of this nature. We may use our section 135 information gathering powers to gather information, if we consider it appropriate.

5.65 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, we may request regular progress updates.

5.66 In cases where the security compromise is not resolved to our satisfaction, we may consider the use of our assessment and enforcement powers set out in sections 105N-P and 105S-V of the 2003 Act.

Inclusion of information on reported compromises in Ofcom's reports

5.67 Ofcom provides periodic reports to the UK Government on the state of the UK's communications infrastructure, in accordance with section 134A and 134AA of 2003 Act. These reports include an annual summary of the security compromises which have been reported to Ofcom. Information about the security compromises reported to Ofcom must be included also in Ofcom's security reports (section 105Z(4)(c) of the 2003 Act).

[29] Cell Data Standard

6. Enforcement

Introduction

6.1 As part of ensuring compliance with the security duties set out under sections 105A to 105D, 105J and 105K, Ofcom is also responsible for the enforcement of such duties.

6.2 Taking action in respect of non-compliance with statutory and regulatory requirements is usually likely to further the interests of citizens and consumers by preventing or remedying consumer harm. It is also important that we take action in an efficient and effective way, that is evidence-based, proportionate, consistent, accountable and transparent, and targeted only at cases where action is needed.

6.3 Information which may trigger an investigation can come to Ofcom's attention from a variety of sources, such as a notification by a provider of a security compromise, routine monitoring and supervision, or because of a complaint. Upon triggering the enforcement process, Ofcom completes an initial assessment in order to determine whether to open an investigation. If an investigation is commenced, Ofcom will rely upon its statutory powers to obtain the information necessary to take appropriate enforcement action. As discussed above, these powers may include: (i) requiring information by issuing s 135 information notices; (ii) directing providers under section 105I to make a statement specifying whether they are acting in accordance with the provisions of the Code; and (iii) issuing assessment notices under section 105O.

6.4 Where we determine that there are grounds for action, we 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, Ofcom will make a final decision on the case. Where appropriate, Ofcom may consider settling a regulatory investigation. Settlement is a voluntary process and leads to a formal, legally binding regulatory decision. Throughout the process, Ofcom may rely upon its new powers (introduced by the Security Act) to require providers to take interim steps or impose a duty to take specified steps by issuing an assessment notice. Ofcom also has a power to deal with urgent cases, including the power to suspend or restrict a provider's activity (section 98).

General approach to investigating compliance and taking enforcement action

6.5 Ofcom's general approach to investigating compliance with or enforcing the regulatory requirements, such as the security duties, is set out in the Enforcement Guidelines[30].

[30] Enforcement Guidelines for Regulatory Investigations. As per paragraph 1.10, in light of the new powers introduced under the Security Act, this guideline is subject to review and an updated draft will be consulted upon by mid-2022.

6.6 In Section 3 above, we provide general guidance about how we envisage exercising Ofcom's powers to issue section 135 information notices, to issue assessment notices and to direct providers to explain any failure to act in accordance with guidance given by the Secretary of State in a code of practice. These powers may be relevant also in relation to Ofcom's enforcement process.

6.7 As explained above (paragraph 3.42), Ofcom will use these powers where we consider it appropriate, reasonable and proportionate to do so.

6.8 Below we set out how we generally expect to exercise our power to impose penalties (section 105T) and our power to direct a provider to take interim steps (sections 105U and 105V). This guidance should be read alongside Ofcom's Enforcement Guidelines and Ofcom's Penalties Guidelines.[31]

Ofcom's power to direct providers to take interim steps (section 105U and 105V)

Legal framework

Three-stage process

6.9 The 2003 Act gives Ofcom the power to impose interim steps to a provider pending the commencement or completion of enforcement action (section 105U and 105V). The process for giving interim directions involves:

- giving a notification setting out the interim steps proposed by Ofcom (section 105U);
- allowing the provider an opportunity to make representations (section 105V(1)(b)); and
- issuing a direction to take interim steps (section 105V).

Notification proposing interim steps

6.10 Ofcom may propose interim steps to a provider only if the conditions set out in section 105U(1) 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 sections 105A, 105B, 105C or 105D;
- Ofcom either has not yet commenced enforcement action (under section 96A) or has commenced but not completed enforcement action (under section 96C(2)(a) or (b));
- 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.

[31] Penalties Guidelines.

6.11 The nature of the "interim steps" which may be required of a provider is set out in section 105U(4). 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

6.12 Ofcom may only direct the provider to take the interim steps once a provider has been given a notification under section 105U, the provider has had an opportunity to make representations about the matters notified, the period allowed for representations has expired (section 105V(1)(c)), and after having considered any representations (section 105V(3)).

Direction to take interim steps

6.13 Ofcom may only direct a provider to take interim steps if we are satisfied that (section 105V(3)):

- 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).

6.14 A direction to take interim steps must include a statement of reasons (section 105V(4)) and specify the time period within which each interim step must be taken (section 105V(5)). A direction cannot require a provider to take interim steps after the completion of enforcement action by Ofcom (section 105V(6)).

6.15 Ofcom must commence or complete enforcement action as soon as reasonably practicable after a direction to take interim steps has been given (section 105V(7)).

6.16 Ofcom may, at any time, revoke or vary a direction to make it less onerous (section 105V(8)).

Ofcom's general policy

6.17 As set out above, Ofcom can impose interim steps under sections 105U and 105V of the 2003 Act only where certain conditions have been met.

6.18 As this power is intended to be used in situations where an actual, or potential, security compromise is serious, we expect to be in close dialogue with the provider to gather the necessary information to inform our decision on whether directing the provider to take interim steps would be appropriate under the specific circumstances.

6.19 After receiving a notification (issued by Ofcom under section 105U) setting out the interim steps proposed by Ofcom, providers will have the opportunity to submit their representations, which we will take into consideration prior to issuing any final directions to take interim steps (under section 105V). Given the urgent nature of a direction to take interim steps, the time given to make representations under section 105U(2)(C) is likely to be short. Our directions will include a statement of our reasons for issuing the direction as well as the time period(s) for completion of the specified interim steps.

6.20 We may issue such a notification and direction to take interim steps before we have commenced enforcement action, up to any point before we have completed enforcement action. Where Ofcom issues such a direction, we must as soon as reasonably practicable commence and complete enforcement action.

Ofcom's power to impose penalties

Legal framework

6.21 For contravention of a security duty (other than the duty to explain a failure to follow a provision in a code of practice under section 105I), Ofcom 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, £100,000 per day.[32]

6.22 For contravention of an information requirement or refusal to explain a failure to follow a provision in a code of practice (under section 105I), Ofcom may impose a penalty up to a maximum of £10 million or, in the case of a continuing contravention, £50,000 per day.[33]

6.23 Ofcom must give providers a period of time to make representations after giving a notification of a penalty before any confirmation decision is made.[34]

Ofcom's general policy

6.24 Ofcom will consider all the circumstances of the case in the round in order to determine the appropriate and proportionate amount of any penalty.

6.25 Ofcom has published penalty guidelines and will have regard to these guidelines in determining the amount of penalty to be imposed under the 2003 Act for contravention of a security duty, a failure to comply with a s 135 information notice or a refusal to explain a failure to follow a provision in a code of practice.

[32] Sections 97, 105S and 105T(1) of the Act.
[33] These maximum amounts are set out in sections 105T and 139ZA of the Act.
[34] Sections 96C(1)(b) and 139A(1)(b) of the Act.

7. Information sharing

Introduction

7.1 The 2003 Act gives Ofcom broad information gathering powers to enable it to monitor and enforce the security framework. Providers are required by law to provide information if asked to do so under these powers. Information collected under these powers may only be disclosed in accordance with the restrictions on disclosure set out in section 393 of the 2003 Act. These restrictions mean that Ofcom will only share information it has received from providers with DSIT, the NCSC, or any other relevant body in a manner consistent with these restrictions.

Legal framework

Statutory gateways under section 393 of the 2003 Act

7.2 Under section 393(1) of the 2003 Act information with respect to a particular business which has been obtained in exercise of powers under the 2003 Act (among others) is not, so long as that business continues to be carried on, to be disclosed without the consent of the person for the time being carrying on that business.

7.3 Section 393(2) sets out a number of exceptions (often referred to as "statutory gateways") enabling the sharing of information without consent. These gateways include any disclosure of information which is made:

- for the purpose of facilitating the carrying out by Ofcom of any of their functions (section 393(2)(a));
- for the purpose of facilitating the carrying out by any relevant person of any relevant function (section 393(2)(b));[35]
- for any of the purposes specified in section 17(2)(a) to (d) of the Anti-terrorism, Crime and Security Act 2001 (c. 24) (criminal proceedings and investigations) (section 393(2)(d));
- for the purpose of any civil proceedings brought under or by virtue of the 2003 Act or any of the enactments or instruments mentioned in section 393(5) (section 393(2)(e));
- for the purpose of securing compliance with an international obligation of the United Kingdom (section 393(2)(f)).

[35] Relevant persons include Ministers of the Crown and the Competition Markets Authority (section 393(3)). Relevant functions include any function conferred by or under the 2003 Act, any function conferred by or under any enactment or instrument mentioned in section 393(5), and any other function specified in an order made by the Secretary of State (section 393(4)).

Other statutory gateways under the 2003 Act

7.4 In addition to the above, further statutory gateways enable the sharing or publishing of information gathered by Ofcom under the 2003 Act. These include:

- section 24B – Ofcom may provide the Secretary of State with any information that they consider may assist the Secretary of State in the formulation of policy;
- section 105L(2) – Ofcom must inform the Secretary of State of the risk/ occurrence of serious security compromises;
- section 105L(3) – Ofcom may inform the Secretary of State of the risk/occurrence of security compromises not caught by duty under section105L(2);
- section 105Z – as noted above, as soon as practicable after the end of each reporting period Ofcom must prepare and send to the Secretary of State a report for the period containing information and advice to assist the Secretary of State in the formulation of policy in relation to the security of public electronic communications networks and public electronic communications services; and
- section 134AB – Ofcom may publish information gathered using our section 135 powers (or information derived from such a process) for the purpose of preparing an infrastructure report under section 134A or 134AA.

7.5 Nothing in section 393 limits, among others, the matters that may be published under section 134AB, prevents the disclosure of information under section 24B or 105L, or prevents the publication or disclosure of a report or part of a report under section 105Z(6).[36]

Section 19 of the Counter-Terrorism Act 2008

7.6 Under section 19 of the Counter-Terrorism Act 2008, a person may disclose information to any of the intelligence services (for example, the NCSC) for the purposes of the exercise by that service of any of its functions. Such a disclosure does not breach any obligation of confidence owed by the person making the disclosure or any other restriction on the disclosure of information (however imposed).

Ofcom's general policy

7.7 Under the telecoms security regime, we expect to need to share certain information to enable Ofcom, the Secretary of State, as the Government policy lead, and the NCSC, with their expertise in the threat landscape, to perform their respective functions, including supporting policy development for telecoms security, helping identify new threats and vulnerabilities, and ensuring that the telecoms security measures set out in Regulations made by the Secretary of State and any codes of practice are keeping up with evolving threats and technologies. Where appropriate, Ofcom may also need to share information

[36] Section 393(6).

with other bodies on an ad hoc basis, such as the Information Commissioner's Office (ICO), to enable them and Ofcom to perform their respective functions.

7.8 Except for some specific circumstances or unless specifically warranted, Ofcom expects to notify providers at the point of formally requesting information of those parts of the information received that will be shared with other bodies and explain the basis for any such disclosure including specifying the relevant statutory gateway Ofcom is relying on. Where appropriate, Ofcom may seek consent from providers to share specific information with other bodies. We anticipate that we will identify the relevant information and set out our approach in our information notices under section 135 of the 2003 Act.

7.9 We set out below more specific guidance on the approach we expect to take in respect of certain types of disclosure.

7.10 The 2003 Act requires us to report to the Secretary of State periodically on infrastructure under section 134A or section 134AA, also known as our Connected Nations reports. The matters that need to be included in our infrastructure reports are set out under section 134B of the 2003 Act. The Security Act expands these matters by requiring Ofcom to report on the extent to which providers of public UK networks and/or services are complying with their security duties.[37] The 2003 Act also requires Ofcom to report to the Secretary of State periodically on matters related to security under section 105Z of the 2003 Act. As part of exercising these reporting functions, Ofcom expects to disclose information gathered from providers under the 2003 Act to the Secretary of State. We expect to adopt the same approach to the sharing of our security report with the Secretary of State as we do in respect of the sharing of our current infrastructure reports, namely to not notify providers of specific information that will be disclosed to the Secretary of State through the security report. Where we intend to publish information related to compliance with the security duties within our Connected Nations reports we will continue to adopt the approach already in place and engage with providers.

7.11 Providers are under a duty to inform Ofcom of any security compromise that has or could have a significant effect or that puts any person in a position to be able to bring about a further security compromise that would have a significant effect (incident report). Ofcom has various functions under the 2003 Act in relation to incident reports, including informing others where there is a risk of a security compromise occurring or a security compromise has occurred. This includes a duty to notify the Secretary of State in certain circumstances and a power to inform various third parties in various circumstances including the Secretary of State, any person who uses or has used the network or service, any provider, any person who makes associated facilities available, any overseas regulator and the European Union Agency for Cybersecurity. Where it is necessary for the exercise of our functions to disclose information from such incident reports to the Secretary of State and/or the NCSC, we expect to disclose the relevant information without prior reference to the provider. Where appropriate we will endeavour to notify the provider after such a disclosure has been made. Where our functions require us to disclose such information to

[37] Section 134B of the 2003 Act as amended by section 105Z(3)(a) and (b) of the Security Act.

parties other than the Secretary of State and/or the NCSC, unless the circumstances require otherwise, we will endeavour to write to providers in advance of making such a disclosure. Where it is not possible or appropriate to write to providers in advance, we will again endeavour to notify the provider after such a disclosure has been made.

7.12 We also expect that Ofcom may need to disclose information to third parties for the purposes of exercising their own functions. We expect that this will include disclosing information to NCSC. Where information is requested by NCSC for the purposes of exercising its own functions, Ofcom expects to disclose such information without prior reference to the provider, although we will explain the likely extent and basis of such sharing when we request the information. To the extent that third parties other than NCSC request that we disclose information for the purposes of exercising their own functions, we will endeavour to write to providers in advance of making such disclosure.

7.13 We expect that Ofcom may also need to disclose information to third parties as part of the exercise of its functions. It may also be necessary for Ofcom to disclose information to the Secretary of State to assist in the formulation of policy. In such cases, we will endeavour to write to providers in advance of making any such disclosures.