Annex 5: Draft 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

DRAFT GUIDANCE:

Publication date: 8 March 2022

Contents

Section

1. Overview 1

2. Introduction 2

3. Compliance monitoring 7

4. Testing 17

5. Reporting security compromises 20

6. Enforcement 26

7. Information sharing 30

Annex

A1. Qualitative criteria and thresholds for reporting security compromises 32

A2. Data to be provided in security compromise notifications 35

A3. Security compromise reporting template 39

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 our 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, provides general guidance on Ofcom's approach to exercising its functions to seek to ensure compliance with the security duties. In particular, it explains the procedures that we are generally expecting to follow in carrying out our monitoring and enforcement activity. It also provides general 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 general 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 general 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.

New legislative framework

2.2 The new legislative framework includes the following elements, which are discussed in more detailed 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)

[1] Section 105A(3) of the 2003 Act goes on to provide a number of exclusions from this definition.

Regulations 2022 (the "Regulations"), which are expected to come into force on 1 October 2022.[2]

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 a code of practice on 1 March 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 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 allows 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 operators to complete system tests, make staff available for interview and permit persons authorised by Ofcom to enter operators' 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

[2] These regulations are still in draft form. DCMS is currently consulting on them.
[3] The Code is still in draft form. DCMS is currently consulting on it.

compromise. In cases of non-compliance, including where a provider has not complied with a notification of contravention, Ofcom can issue financial penalties. These powers are set out in more detail in section 3.

Reporting functions

2.12 Ofcom also has certain reporting functions 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 sections 134A which include the extent to which providers are complying with the security duties.[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 (starting from two years after commencement, i.e. expected to be from October 2024[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 will be able to publish these reports or extracts from them.[6]

[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] In accordance with section 28(2)(b) of the Security Act, this date is subject to the commencement date that will be specified by the Secretary of State in regulations.
[6] Section 105Z(6)-(8) of the 2003 Act.

Infrastructure reports

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[7].

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 DCMS 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 will therefore work with these two organisations as the new framework is implemented. This includes 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:

- compliance monitoring (section 3);
- testing (section 4);
- reporting security compromises, both to Ofcom and to users (section 5 and annexes A1-A3);
- enforcement (section 6);
- and about Ofcom's approach to sharing information with other relevant public bodies (section 7).

[7] See our Connected Nations and infrastructure reports.

3. 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 general process for identifying into which "tier" (as described in the Code) each provider falls, before going to on to provide general 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 statutory information gathering powers under section 135 of the 2003 Act.

Principles behind Ofcom's approach to compliance monitoring

A supervisory model

3.3 The Security Act introduces 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, 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 We recognise that the new framework will require an ongoing compliance journey for providers. Firstly, many providers are likely to need to make significant changes to their existing security practices in order to fully comply with the framework. In DCMS' Supply Chain Review, Government expressed the view that the level of security within the sector needed to be improved and that the new framework would facilitate this. Given the scale and complexity of many providers' operations, it is likely to take time to fully achieve this improvement.

3.6 Secondly, the threats faced by communication providers are continually changing as technologies evolve and attackers learn and become more sophisticated. A provider's work on security is therefore never complete and requires a strong internal security culture leading to continuous improvement.

3.7 A key objective of our monitoring role over the first few years of the regime is therefore to determine if each provider is implementing appropriate organisational and technical measures with sufficient pace, as they continue to work towards full compliance. Where

we find areas of concern, we will seek to work with providers to ensure appropriate and proportionate measures are implemented in accordance with the security duties. We expect that this collaborative approach will foster more compliant behaviours, reduce the volume of breaches under the 2003 Act, as well as reducing the need for regulatory investigations. As necessary, we will also stand ready to engage our suite of enforcement powers. Our approach to enforcement is set out in Section 6.

Compliance monitoring based on tiering

3.8 Although certain 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 UK's major fixed and mobile providers whose availability and security is likely to be critical to consumers and businesses in the UK.
- Tier 2 (relevant turnover of £50m-£1bn): Medium sized providers who are likely to be critical to regional and business connectivity. The Code indicates that these providers should be given 2 years longer than Tier 1s to implement the measures it contains.
- Tier 3 (relevant turnover below £50m): This is the long tail of smaller providers, including small and micro businesses. Although the overarching duties in the Act apply to all such companies, micro-entities are exempt from the Regulations.[8] Furthermore, the Code does not apply to any Tier 3 providers. For further details on the Government's proposed tiering system, see the Government's consultation.

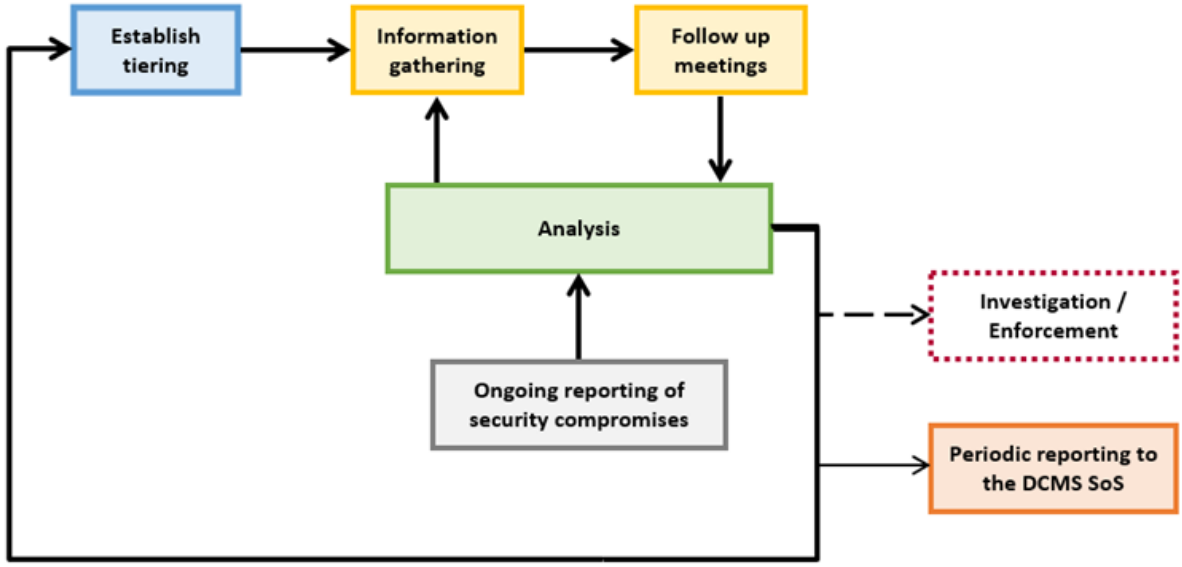
Our approach to monitoring Tier 1 and Tier 2 providers

3.9 Consistent with the approach taken in the Code and reflecting our proportionate approach to compliance monitoring, balancing the need for security with the size and criticality of the networks and services involved, our proactive compliance monitoring activities will be on providers in Tiers 1 and 2. The rest of this section explains how we intend to approach this monitoring.

3.10 Due to the nature of the framework, providers' implementation of measures will evolve and we will expect to understand more about their networks, services, and compliance approaches over time. For this reason, we see both compliance and regulation as an ongoing cyclical journey, which will ramp up over time, rather than a linear process. An overview of our planned approach for the first few years is shown and discussed below:

[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: Compliance monitoring approach for Tiers 1 and 2



Establish tiering

3.11 Ofcom will confirm which tier providers are in, using the thresholds in the Code.

3.12 We already collect data on relevant turnover from providers each year, for the purpose of setting our annual administrative charges. Therefore, to the extent we might already hold this data, where it is relevant for establishing which tier a provider falls into, we would expect to seek permission from providers to use this data. In future years, we expect to expand the purpose for which we collect data to include for the purpose of establishing tiering.

3.13 Following our analysis of this data, we then expect to inform those providers falling in Tier 1 and Tier 2, and seek to hold an introductory meeting to discuss our approach to compliance monitoring. We do not expect to inform or meet with providers falling into Tier 3, so any providers who do not hear from us can assume they will not be part of the Tier 1 and Tier 2 compliance monitoring set out in this guidance. However, they 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.

3.14 While we would expect to complete the process for establishing tiering within 3 months of the framework coming into force, it may take longer as the timing will depend on the information we receive from relevant providers.

3.15 Following this initial tiering notification process, we will continue monitoring each provider's relevant turnover annually to check whether any have moved into a different tier. We will assess any movement between tiers in accordance with the guidance in the Code.

Information-gathering powers (section 135)

Legal framework

3.16 Ofcom has broad information gathering powers under section 135 of the 2003 Act which allow 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));

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.

3.17 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

3.18 It is our intention to rely primarily on information notices issued under section 135 of the 2003 Act ("s135 information notices") to build our initial understanding of each provider's compliance with the security duties and their adherence to any codes of practice, including the Code. Where necessary, we have a range of other powers we can use to collect additional information about compliance, such as assessment notices (section 105O-Q) and notifications directing a provider to give a statement to Ofcom explaining whether they have failed to act in accordance with guidance given by Secretary of State in a code of practice and why (section 105I).

3.19 Collecting information about the wide range of security duties and measures covered by any regulations and codes of practice is a new exercise for both Ofcom and providers. In

line with our general policy on information gathering,[9] where timescales allow and it is appropriate to do so, we will send draft s135 information notices to providers for comment before finalising them. In particular, we would normally expect to send the notices in draft form when we gather information to conduct regular monitoring activity. We expect we will have to refine the process as we gain experience, such as the level of detail required, and the extent of information we gather in any given notice.

3.20 In order to assess the measures taken by a provider, Ofcom will request a detailed picture of the networks and services in scope of the security duties, and the various functions and assets they comprise. As an example, we will need to understand the provider's full range of "security critical functions" (as defined in the Regulations), and which of these are "network oversight functions" (as defined in the Code), in order to go on to assess whether appropriate measures are being taken to protect each of them. Building this picture will therefore form an important objective of our early information requests.

3.21 Subsequently, the bulk of the s.135 information notices will be concerned with understanding the measures each provider has in place in order to meet its obligations. We are required to take into account relevant provisions in any code of practice when assessing compliance,[10] so the information we request will be primarily intended to help us establish (i) the extent to which the measures the provider has in place, or is planning to put in place, align with those in any codes of practice, including the Code and (ii) any alternative or additional measures which providers might take to comply with their security duties. Alongside asking about the measures a provider has in place, we may also ask for relevant documentation or other information describing or demonstrating a measure.

3.22 Ideally, we would gain a full picture of all the relevant measures being taken or planned by a provider from the outset. However, given the scope and scale of the regime, including the Regulations and the Code, we anticipate that we will put in place a rolling programme of information requests. More information on how we expect this to be structured is included below.

3.23 The Code itself sets out a series of dates spanning from 2023 to 2028, reflecting Government's expected timescales for implementing the different measures contained in the Code. We therefore expect to broadly align the order in which we request information about measures with the relevant dates set out in the Code. An objective of the monitoring process is to gather information about the implementation of each of the measures in the Code, and any alternative or additional compliance measures a provider is taking, well in advance of these dates wherever possible. This will allow us to track progress and give an early warning of any potential compliance concerns.

3.24 In addition to issuing s135 information notices as part of our regular monitoring activity, where we have concerns about compliance, it may also be appropriate to use other powers to gather information that will inform our enforcement activity. As mentioned

[9] See Ofcom's policy statement on information gathering.
[10] Section 105H(3) of the 2003 Act.

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).

3.25 The information that we gather from providers will also be used to assist us in preparing our security report to the Secretary of State.

Information-gathering programme

3.26 As noted above, we expect the detail of our information gathering approach to be refined over time. However, our current, tentative expectations for the overall shape of the programme are as follows:

Tier 1 providers

- Establish that the provider is in Tier 1 (3 months)
- Initial s135 information notice, covering networks/services/assets in scope and an initial number of Code measures. We expect this to take around 4 months
- Subsequent s135 information notices:
  - Approximately one every six months
  - Allowing four months for the provider to reply
  - We expect to need at least four of these subsequent s135 information notices, in order to gather a reasonable level of detail about all Code measures, while keeping the size of each request manageable

Tier 2 providers

- Establish that the provider is in Tier 2 (3 months)
- Initial s135 information notice, covering networks/services/assets in scope and an initial number of Code measures. We expect this to take around 6 months
- Subsequent s135 information notices:
  - Approximately one every nine months
  - Allowing six months for the provider to reply
  - We expect to need at least four of these subsequent s135 information notices, in order to gather a reasonable level of detail about all Code measures, while keeping the size of each request manageable

3.27 This approach may 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

3.28 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 s135 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.

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

Legal framework

3.29 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)).

3.30 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

3.31 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.

3.32 As explained above, it is our intention to rely primarily on s135 information notices. As part of this, our routine monitoring will ask providers for information relevant to assessing whether they are complying with their security duties, taking into account any relevant provisions set out in any codes of practice, including the Code. Where this or other information gives us reasonable grounds to suspect providers are not acting in accordance with any such code, we may use our s.105I powers. We will use the information provided to inform our compliance assessments and when considering any subsequent enforcement action.

3.33 In practice, we expect providers to engage constructively with our routine monitoring processes and provide a clear picture of the steps they are taking towards compliance

when providing information in response to our s135 information notices. Therefore, we only anticipate using our s105I power where we consider that a clear statement from a provider of the type required under s105I 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

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

3.35 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.

3.36 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 (s.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 (s.105O(2)(b));
- make people available for interview (s.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 (s.105O(2)(d)-(k)) (this power of entry is discussed in more detail in the "Power to enter premises" section below).

3.37 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.

3.38 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

3.39 As noted above, there may be circumstances where the use of our broader suite of powers under the 2003 Act, such as the power to issue assessment notices under s105O or s105P, 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.

3.40 While we expect to gather the majority of information through our routine monitoring using s135 information notices, we may, in some circumstances, decide it is appropriate for us to use an assessment notice to inform our assessment of a provider's compliance with their security duties. During the early years of the framework, while we are conducting the programme of s135 information notices set out above, we are not planning routinely to use assessment notices. We will keep this position under review and update this guidance as necessary.

3.41 We recognise that complying with an assessment notice may require more substantial effort or additional costs for providers than responding to our s135 information notices or providing a statement in response to a s.105I notice. The decision to issue an assessment notice is therefore likely to indicate an escalation in our concerns around compliance that has not been resolved through routine engagement.

3.42 Where appropriate, we may also use assessment notices to inform our enforcement activity.

3.43 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

3.44 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")[11] to enter non-domestic premises[12] for various purposes. Specifically:

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

- 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));
- 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

3.45 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

3.46 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.

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 (s.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 (s.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)).[13]

Ofcom's general policy

Voluntary testing

4.5 As clarified in the Explanatory Notes accompanying the Security Act,[14] the tests required by an assessment notice may include 'penetration testing' and 'red teaming exercises'. Ofcom will continue to run its voluntary red-team style, penetration testing (TBEST) alongside our expanded powers.

[13] In addition, regulation 14 of the Regulations specifies further measures which providers should take in relation to testing. Specifically, providers are required to carry out (or arrange for a suitable person to carry out) at appropriate intervals, such tests in relation to the network or service as are appropriate and proportionate for the purpose of identifying the risks of security compromises occurring in relation to the network or service. See regulation 14 for further details.

[14] Paragraph 107 of the Explanatory Notes accompanying the Security Act.

4.6 TBEST has been used by providers since 2018 in collaboration with DCMS, the NCSC, and Ofcom. TBEST is undertaken with technical and tactical advice from the NCSC and strategic input from DCMS. Its aim is to check on the effectiveness of a provider's security controls, processes, infrastructure, software, policies and employee behaviors, to protect its critical networks or services from a cyber-attack.

4.7 It simulates an advanced attack against a provider's critical infrastructure and assets, 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).

4.8 The tests target several "flags" that are agreed beforehand (between provider, the NCSC and Ofcom) that are indicators of a compromised critical asset (without necessarily accessing the critical asset). For example, if testers have gained access to "privileged access management" platforms, used to access the core-network elements, then it is assumed that the core network elements would have been compromised and the testers do not need to go ahead and access the core network elements.

4.9 The test is done by an independent penetration testing company. They use Open-Source Intelligence (OSINT) to profile the critical assets, as well as the employees and third parties who may access them.

4.10 They will then use similar tactics and methodologies as a real well-resourced attacker. For example, they will send phishing e-mails to targeted employees, use lateral movement to get onto additional assets within the corporate network (that may facilitate access to the critical infrastructure).

4.11 At the end of the testing, the penetration testing company will produce a report and present the findings back to the provider, the NCSC, and Ofcom. The provider then develops a mitigation plan to address the findings and works with Ofcom and the NCSC to approve and monitor the roll-out of the plan.

Testing required under the new framework

4.12 A provider who undergoes TBEST is showing security maturity in wanting to understand the effectiveness of its security program and security controls that are in place to prevent and detect such attacks. TBEST will show the real-life improvements in security due to the providers roll-out of security programs and security improvements. Under regulation 14 of the Regulations, providers are required to carry out regular testing for the purpose of assessing the risk of security compromises occurring in relation to their network or service, in a manner similar to TBEST.

4.13 There are other kinds of testing besides TBEST (or red-teaming), which are more targeted in scope and techniques, that providers do undertake. Though not looking to simulate a real-life attacker, they do provide valuable information on weaknesses and vulnerabilities

within the scope of the test. Testing like this is often a requirement for compliance regimes like the Payment Card Industry Data Security Standard (the "PCI-DSS").

4.14 In our experience, voluntary participation by providers generally leads to greater input and engagement showing an understanding of the value of testing. Therefore, as stated previously, we will continue to run TBEST as a voluntary, open, and collaborative program with providers. However, where appropriate, we may exercise our statutory powers to require a provider to undergo testing, either like TBEST or some other types of testing.

4.15 We would expect to use such mandated testing in order to obtain assurance that measures a provider states as being implemented, appropriately reduce the likelihood or impact of a real-life cyber-attack. The results of these tests may therefore form part of Ofcom's assessment of a provider's compliance with its security duties. We would expect that it is less likely that testing under s105O will be required if a company undertakes periodic voluntary TBEST, as this attempts to test the effectiveness of the totality of all security controls currently in place, and can therefore give Ofcom significant insight into the overall effectiveness of a provider's security.

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.

Duty under s105J to inform users of risk of security compromise

Legal framework

5.2 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 (s.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 (s.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

5.3 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.

5.4 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?

5.5 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. 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.

5.6 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 moving to an alternative provider.

5.7 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.

5.8 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 s105K

Legal framework

5.9 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.

Ofcom's general policy

Reporting of network or service outages

5.10 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 105(2)(a)). This requirement effectively replaces the reporting duty in s105B of the 2003 Act prior to its amendment by the Security Act, under which providers reported incidents which caused disruption, or 'outages', to end user services. We expect the majority of these sorts of network or service outages, often known as 'availability' or 'resilience' incidents, to continue to be reported to Ofcom under this new requirement. Further guidance on our expectations for such reporting is set out below.

Reporting of other security compromises

5.11 As stated above (paragraph 2.4), the definition of security compromise in section 105A(2) also 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.

5.12 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.

5.13 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".

5.14 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.[15] 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. For the avoidance of doubt, we consider that providers should report the initial security compromise to Ofcom even if they consider that a further attack would be unlikely to succeed, due to the defences they have in place.

General comments on reporting security compromises to Ofcom

5.15 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.

[15] As clarified in paragraph 86 of the Explanatory Notes accompanying the Security Act, section 105K(1)(b) is intended to ensure that providers report to Ofcom those attacks that do not at the time of the attack affect the network or service, but allow access to a network that could result in future security compromises.

5.16 In relation to the initial notification of a security compromise requiring urgent action (an "urgent compromise," discussed further below), 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.

How providers should report security compromises

5.17 Initial notifications about urgent security compromises should be made via an agreed contact, or the 24/7 reporting number outside of office hours. This should then be followed by a normal security compromise report as set out below.

5.18 All security compromise reports should be submitted to incident@ofcom.org.uk

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

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

When providers should report security compromises

5.21 We expect providers to make initial notifications of urgent security compromises as soon as possible, and usually within 3 hours of the provider becoming aware of them.

5.22 We expect other security compromises to be reported within 72 hours of the provider becoming aware of them.

5.23 Where a provider has a significant number of 'non major' security compromises (typically those meeting only the lowest fixed numerical threshold), they may be excluded from the 72 hour reporting requirement above, and instead reported in batches.

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

5.25 To facilitate Ofcom's annual reporting, providers should keep data for security compromises that have been reported for no less than 18 months following incident resolution.

What should be reported

5.26 Section 105K(2) requires providers to take account of a number of factors in determining whether the effect of 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. In particular, 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."

5.27 The qualitative criteria and numerical thresholds set out in Annex 1, which we have developed taking into account the factors listed in section 105K(2), set out our view of the level at which security compromises are likely to be significant and should therefore be reported to Ofcom. In doing so, we are also providing guidance on the types of compromises that we would normally expect to require urgent action.

5.28 If any one of the criteria or thresholds is met, the provider should submit a security compromise report. We would expect that providers will not adopt an unduly restrictive approach to interpreting these criteria – if there is doubt as to whether a particular criterion is met, providers should submit a report. Ofcom has the power to take enforcement action where providers do not report in accordance with the statutory requirements.

Data to be provided

5.29 The information that we expect to receive from providers where they are required to report a security compromise is set out in Annex 2.

Report format

5.30 Annex 3 provides a reporting template.

Follow up actions or requirements in response to a security compromise

5.31 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.

5.32 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 an incident follow up meeting.

5.33 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.

5.34 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.

5.35 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.

Ofcom's reports under sections 134A and 134AA

5.36 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.

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 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[16].

[16] 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 s135 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.[17]

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.

[17] 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. [18]

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. [19]

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. [20]

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 guidelines on its approach to penalties 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.

[18] Sections 97, 105S and 105T(1) of the Act.
[19] These maximum amounts are set out in sections 105T and 139ZA of the Act.
[20] 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 is subject to the restrictions on disclosure set out in section 393 of the 2003 Act. These restrictions are designed to give comfort to providers that Ofcom will only share information it has received from operators with DCMS, the NCSC, or any other relevant body in certain specific circumstances.

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));[21]
- 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)).

[21] 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.

Section 19 of the Counter-Terrorism Act 2008

7.5 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

7.6 Under the new regime, we expect to need to share certain information to enable Ofcom, DCMS, 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 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.

7.7 Unless specific circumstances justify a different course of action, 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.

A1. Qualitative criteria and thresholds for reporting security compromises

Qualitative criteria

Urgent security compromises

A1.1 Security compromises should be notified as "urgent" if they meet any of the following criteria:

- All security compromises involving major cyber security breaches that are reportable under the "Reportable security compromises" criteria below.
- Security compromises affecting services to 10 million or more end users.
- Security compromises affecting services to 250,000 or more end users and expected to last 12 hours or more.
- Security compromises attracting national mainstream media coverage.
- 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 single security compromise that affects the provision of wholesale services to both fixed and mobile communications providers.

A1.2 Notification of urgent security compromises should be made direct to the 24 hour Incident Reporting number: 0207 981 3184.

Reportable security compromises

A1.3 Reportable security compromises are as follows:

General

- Any security compromises meeting the thresholds set out in Table 1 and/or Table 2 below.
- 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 security compromises involving major cyber security breaches, which meet any of the criteria in this list.

Repeat incidents

- Repeat incidents are considered to be those which reoccur within four weeks, or are separate incidents affecting the same services in the same areas over a four-week period.

- For repeat incidents, the provider should combine the impacts of the individual incidents in determining whether they meet the numerical thresholds.

Outages affecting the ability of a user to contact the emergency services

- 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 has a link to a potential loss of life.

Fixed network numerical thresholds

Table 1: Fixed network numerical thresholds

Network/service type	Minimum number of end customers affected [1]	Minimum 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
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 incident.*
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.*

Mobile network numerical thresholds

Table 2: Mobile network numerical thresholds

Network/service type	Minimum number of end customers affected[1]	Minimum duration of service loss or major disruption
Mobile network providing access to the emergency services [2]	1,000	1 hour
Mobile network providing access to the emergency services [2]	100,000	Any duration
MVNO voice or data service/network offered to retail customers [3]	25% [4]	8 hours

Notes on Table 2:

1. *A customer is affected if the main functions of a network or service are not available to them due to the incident.*
2. *Where a provider expects emergency roaming will have allowed customers in the affected area to retain 112/999 access, it is not required to report the incident under this threshold.*
3. *A Mobile virtual network operator (MVNOs) should report incidents affecting its end customers, even where incidents 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.*
4. *This threshold should be interpreted as 25% of the provider's total number of end customers on the affected service.*

A2. Data to be provided in security compromise notifications

Data required

Urgent compromises – initial notification

A2.1 For "urgent compromises", providers should inform us as quickly as possible and usually within 3 hours of the provider becoming aware of them. We expect this initial notification to simply acknowledge that the provider is aware of a major incident, and give an indication of its nature. Any other information that is readily available will be welcomed.

Incident reports

A2.2 All other incident 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 template in Annex A3. Where full or final information is not available at the time of reporting, updated reports can be provided as further information becomes available.

1. Provider name

A2.3 The full name of the communications provider.

2. Provider incident reference number

A2.4 A unique reference number that can be used to identify the incident in communications with the provider.

3. Date and time of occurrence

A2.5 The date and time that the incident commenced formatted as : dd/mm/yyyy hh:mm

4. Date and time of resolution

A2.6 The date and time that the incident was resolved completely formatted as : dd/mm/yyyy hh:mm. Where the incident is ongoing at the time of reporting, the resolution time may be provided when it is available.

5. Location

A2.7 Location information should describe the geographical location of the impact of the incident. Where possible, a UK postcode should be provided which identifies the geographical area where service interruption was experienced.

A2.8 Where the geographical impact of an incident 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.

A2.9 Where an issue has regional or national impact, the provider should provide the name of the region or nation in lieu of a postcode.

A2.10 In the case of mobile incidents 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.

A2.11 Use the following examples as a guide:

Table 3: Providing location information

Failure location examples	Location expectation
Service interruption due to failure at a single or small number of cell sites	The full post code of the cell site(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 'LS1' would be appropriate.
Service interruption with impact across the whole of Manchester	In this case the CP should report the location as 'Manchester'.
Service interruption with impact across an entire county/region	In this case the CP 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.

6. Brief description of incident

A2.12 Provide a short summary of the incident, including any relevant information not captured elsewhere on the template.

7. Impact

Services affected

A2.13 Provide full details of the services affected. This should identity services as understood by the subscriber, for example telephony, broadband, 2G, 3G, 4G, 5G etc.

Number/proportion of users affected

A2.14 Provide details of the number of subscribers affected by the incident. 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 the provider's end customers for this service that this represents.

A2.15 The provider should provide details of the total number of affected customers against every service associated with an incident, even where that service did not meet specific thresholds. For example, for an incident which exceeds a voice threshold and also affects data customers – but does not exceed a data threshold – the number of data end customers affected should be included in the report.

A2.16 Where the impact of an incident varies over time, effort should be made to explain how this was the case.

A2.17 Where exact numbers are not available (for example due to a mobile cell site failure), we expect the provider to use historical data to estimate the number of end customers affected.

A2.18 Providers which offer wholesale products to other providers may have little or no visibility of the number of end customers affected by an incident 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 an incident is likely to result in service loss to end customers which will exceed the reporting thresholds, we would encourage them to report this.

A2.19 A provider should report qualifying incidents 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 incidents affecting such additional services.

Networks and assets affected

A2.20 The provider should provide an overview of the networks and assets that were affected during the incident. At this stage the overview should be brief. If we decide to investigate the incident further, network and asset information may be required to a level of detail commensurate with the following:

- legacy networks and services – ENISA Technical Guideline on Threats and Assets (Section 5)
- virtual / 5G networks and services – ENISA 5G Networks Threat Landscape (Section 5)
- access / aggregation and full-fibre networks – Ofcom's 2021 WFTMR (annexes 2 and 26).

Fixed and mobile

A2.21 The provider should indicate if this incident has had an impact on both fixed and mobile networks or services.

8. Summary of incident cause and action taken so far

A2.22 The provider should provide sufficient detail to enable us to classify the incident against one of the root cause and primary cause categories defined in the current ENISA Technical Guideline on Threats and Assets.

A2.23 The provider should provide details of action taken to manage and remedy the incident, and any measures taken to mitigate the risk of reoccurrence.

9. Third party details

A2.24 If the cause of the incident was the failure of a third party service, provide the name of the third party.

A2.25 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

A2.26 Details to enable us to follow up on the incident if required.

A3. Security compromise reporting template

1. Provider name	
2. Provider incident reference number	
3. Date and time of occurrence	*dd/mm/yyyy hh:mm*
4. Date and time of resolution	*dd/mm/yyyy hh:mm*
5. Location	
6. Brief description of incident	
7. Impact: **a) Services affected** **b) Number/proportion of users affected** **c) Networks and assets affected** **d) Fixed and mobile**	
8. Summary of incident cause and action taken so far	
9. Third party details	
10. Name and contact details for follow up	