EXPLANATORY NOTES

Telecommunications (Security) Act 2021

Chapter 31

£11.50

TELECOMMUNICATIONS (SECURITY) ACT 2021

EXPLANATORY NOTES

What these notes do

These Explanatory Notes refer to the Telecommunications (Security) Act 2021 (c. 31) which received Royal Assent on 17 November 2021.

- These Explanatory Notes have been prepared by the Department for Digital, Culture, Media and Sport in order to assist the reader in understanding the Act. They do not form part of the Act and have not been endorsed by Parliament.
- These Explanatory Notes explain what each part of the Act will mean in practice; provide background information on the development of policy; and provide additional information on how the Act will affect existing legislation in this area.
- These Explanatory Notes might best be read alongside the Act. They are not, and are not intended to be, a comprehensive description of the Act.

Table of Contents

Overview of the Act

1 The Telecommunications (Security) Act ("the Act") takes forward the Government's commitment published in the 2019 *UK Telecoms Supply Chain Review Report* to introduce a new security framework for the UK telecoms sector to ensure that public telecommunications providers operate secure and resilient networks and services and manage their supply chains appropriately.

2 The Act amends the Communications Act 2003 by establishing a new telecommunications security framework, including new security duties on public telecommunications providers and new powers for the Secretary of State to make regulations and issue codes of practice. It includes provisions strengthening Ofcom's regulatory powers, allowing them to enforce the new framework.

3 The Act also introduces new national security powers for the Government to impose, monitor and enforce controls on public communications providers' use of designated vendors' goods, services and facilities within UK telecommunications networks.

4 In the previous parliamentary session, the Act completed Committee stage in the House of Commons before it was carried over.

Policy background

5G and Full Fibre networks

5 As outlined in the 2018 *Future Telecoms Infrastructure Review*, the widespread deployment of 5G and full fibre networks is a primary Government objective. These networks will help to drive future economic growth, enabling a wide range of new products and services that require faster speeds and more processing power. 5G has the potential to connect a vast network of people, objects and communication systems, including those within critical sectors.

6 The development of 5G and full fibre networks also creates new security challenges. The speed, scale and processing power of the UK's future digital infrastructure will create new economic and social opportunities for greater connectivity, including across the UK Critical National Infrastructure (CNI) sectors that are likely to have a greater dependence on 5G infrastructure compared to that of legacy arrangements (2G/3G/4G). The technical characteristics of 5G networks increase their risk profile compared to previous generations of networks. 5G networks will run at much faster data speeds and will be based on software running on commodity hardware, rather than proprietary hardware. Over time, to achieve the full potential of 5G, some of the 'core'[1] functions will move closer to the 'edge'[2] of the network. As this happens, it will be necessary to ensure security arrangements are able to protect both the edge and core of the network.

7 The security of telecoms infrastructure needs to be considered within an international context. Certain state, state-sponsored and other actors have the intent and capability to carry out espionage, sabotage and destructive or disruptive cyber-attacks, including through access to

1 The 'core' includes critical functionality (e.g. user authentication and call routing).

2 The 'edge' includes local aggregations sites (i.e. data nodes in metropolitan areas) which are closer to end-users.

the telecoms supply chain. Since 2017, the UK Government has, based on National Cyber Security Centre (NCSC) assessments, attributed a range of malicious cyber activity to Russia and China, as well as North Korean and Iranian actors.

The Office of Communications (Ofcom)

8 Ofcom is the independent regulator for communications in the UK. Its remit covers the regulation of broadband and telecoms, TV, radio, video-on-demand services and postal services. It is also responsible for the effective management of use of the radio spectrum.

9 Ofcom is established under the Office of Communications Act 2002. Ofcom's powers are found in the Communications Act 2003 and the Wireless Telegraphy Act 2006, as well as other enactments including the Broadcasting Acts 1990 and 1996, and the Postal Services Act 2011.

10 Ofcom is a statutory corporation. Its governance arrangements are set out in the Office of Communications Act 2002 and as a public authority it is also subject to other legal duties, including requirements to ensure it acts compatibly with human rights (under the Human Rights Act 1998) and complies with data protection legislation. The Act does not affect those obligations.

The Communications Act 2003

11 The Communications Act 2003 ("the 2003 Act") provides the current regulatory framework for telecommunications security. The responsibility for the management of security and resilience risks for UK telecoms is shared between Government, Ofcom and industry. The 2003 Act, as amended by the Electronic Communications and Wireless Telegraphy Regulations 2011, requires public telecommunications providers to take measures to protect the security and resilience of their networks and services, and gives Ofcom enforcement powers. The relevant provisions are found at sections 105A to 105D of the 2003 Act.

The UK Telecoms Supply Chain Review

12 In 2018-2019, the Government carried out a review of UK telecoms networks' supply chain arrangements. Conclusions of the review were published in the *UK Telecoms Supply Chain Review Report* in July 2019.

13 The Review identified that inadequate industry security practices were driven by a lack of incentives to manage risk, including the inability of the regulatory framework to drive improvements in cyber security. It concluded that higher standards and practices of cyber security are required across the telecoms sector as a technical pre-condition for secure 5G and full fibre networks.

14 The Review called for a new, more robust telecoms security framework, that will meet security challenges both now and in the future whilst ensuring the timely roll-out of the UK's critical digital infrastructure. It suggested that as technologies grow and evolve the UK must have a security framework that is fit for purpose and ensures the UK's telecoms critical national infrastructure remains safe and secure both now and in the future.

15 The *UK Telecoms Supply Chain Review Report* explained that the Government would establish a new robust security framework for the UK telecoms sector, marking a significant shift from the current model. The new framework is necessary to safeguard the UK's national security interests and will build on existing capabilities. It will provide clarity to industry, whilst providing the necessary flexibility and powers for the Government to respond appropriately as risks, threats and technologies change.

16 The Report also explained that the Government would create new powers to manage the risks posed by high risk vendors. High risk vendors are those who pose greater security and

resilience risks to UK telecoms networks. This new framework will help to ensure that telecoms providers are managing the security risks posed by all suppliers.

17 The final conclusions of the Review, which were agreed by the National Security Council in January 2020, set out the need for new national security powers to control the presence of high risk vendors in UK networks.

High Risk Vendors

18 On 28 January 2020, in light of detailed technical and security analysis provided by the National Cyber Security Centre (NCSC), part of GCHQ, the Government announced that new restrictions should be placed on the use of 'high risk' vendors in the UK's 5G and full fibre networks. It announced that such vendors should be:

- excluded from security critical network functions;
- excluded from sensitive geographic locations; and
- restricted to a minority presence in other network functions to a cap of up to 35%, subject to an NCSC-approved risk mitigation strategy.

19 The Government stated in January 2020 that the NCSC would continue to review and update its advice as necessary. On 15 May 2020, the US Department of Commerce announced that new sanctions had been imposed against Huawei through changes to the foreign direct product rules. The new US measures restrict Huawei's ability to produce essential components using US technology or software. The NCSC reviewed the consequences of the US actions, and reported to Ministers that they had significantly changed their security assessment of Huawei's presence in the UK 5G network. The NCSC concluded that given the uncertainty the US sanctions created around Huawei's supply chain, the UK could no longer be confident it would be able to guarantee the security of future Huawei 5G equipment affected by the change in the US foreign direct product rules. To manage this risk, the NCSC issued new advice to the Government on the use of Huawei in the UK telecoms network.

20 The Government agreed with the NCSC's advice, that to secure the UK's public telecoms, providers should not use Huawei equipment affected by the US sanctions to build the UK's future networks. Consequently, on 14 July it announced that public telecoms providers should:

- stop purchasing affected 5G equipment from Huawei after 31 December 2020; and
- remove all Huawei equipment from 5G networks by the end of 2027.

21 The Government advised full fibre telecoms providers to transition away from purchasing Huawei full fibre equipment affected by the US sanctions. A technical consultation would determine the precise timetable from which point full fibre telecoms providers should stop procuring affected equipment.

22 The NCSC currently provides advice to public telecoms providers on the risks presented by high risk vendors and on the measures that the NCSC recommends they adopt as a result. The Act provides the Government with powers to impose binding controls on public communications providers' use of high risk vendors.

Telecoms Security Framework

Responsibilities of Telecoms Providers

23 The Government plans to provide the UK with one of the most robust telecoms security frameworks in the world. Telecoms companies – providers of public electronic communications networks and services (see definitions in Annex A) – are already required to implement general security protections under the existing 2003 Act provisions. The Government intends to build on these practices to remedy the flaws identified in the *Telecoms Supply Chain Review*.

24 To do this, the Act sets out new duties on telecoms providers to raise the bar for security. It requires telecoms providers, overseen by Ofcom, to design and manage their networks to protect against existing and future threats to the UK's network security. This means identifying, reducing and eliminating risks to networks and services. Public telecoms networks and services will be protected by the provider safeguarding their availability and confidentiality, and making them secure from unauthorised interference.

25 Where security compromises do occur, the impact on end-users can be substantial and potentially damaging. The Act therefore places duties on providers to take appropriate and proportionate action to ensure that the effects of compromises are limited, and to act to remedy the impact on networks and services.

26 While networks are owned and operated by different companies, there are common measures that can be taken to level up security protections across all networks and services. Analysis was conducted during the *Telecoms Supply Chain Review*, including in-depth contributions from and interviews with telecoms providers, vendors and other industry representatives. This engagement, plus the practical findings of threat-based, intelligence-led penetration testing and industry-submitted reports of breaches, identified the areas posing greatest risk to networks and services. This has been supplemented by NCSC threat analysis that determines the security outcomes most needed to prevent security flaws.

27 The Act makes provision for the Secretary of State to make regulations, setting out common security outcomes and the actions to be taken to meet them. This includes the ability to make regulations that provide for measures to be taken to prevent security compromises, and – where specific compromises are detailed in the regulations – measures to remedy the effects of compromises on the network or service. Such regulations may include, for example, specific security requirements that ensure networks and services are securely built, managed and overseen, and that vendor procurement and ongoing management support security.

28 The UK has a competitive telecoms market which spans large, multinational companies through to small and micro businesses. Reflecting this diversity, Ofcom as the communications regulator and NCSC as the expert technical security authority provide support and advice, tailored to different types of provider, on appropriate detailed measures to secure their networks and services. The Government therefore recognises that guidance can provide clarity and certainty to providers for achieving compliance with legal obligations. The Act makes provision for the Secretary of State to issue a new telecoms security code of practice, that will set out to certain types of provider the detailed and specific security measures they should take to comply with the law. These codes will be based on NCSC best practice security guidance, and the Government will consult publicly on their initial implementation and subsequent revision. The codes of practice will be admissible in legal proceedings, and a court or tribunal must consider them where they are in force and where a provision is relevant to the proceedings.

29 The European Electronic Communications Code Directive (EECC) included provisions relating to telecoms security. Some of these reflected the previous EU framework for electronic communications and were already transposed in UK law. Others are being given effect through the Act. These address the obligations on providers to report a range of security incidents to Ofcom. This will give Ofcom the information that they need to understand security across the industry.

Ofcom's Regulatory Powers

30 The Act will provide Ofcom with stronger regulatory powers to enforce the new regime. It sets out new responsibilities for Ofcom to assess providers' security. Ofcom has a power, going beyond the current audit powers, to issue assessment notices. These will allow Ofcom to assess, or commission others to assess, providers' compliance. In completing these assessments, Ofcom will take into account any relevant code of practice. Ofcom will be able to complete audits of providers' security provisions and technical tests of a provider's security, as well as require providers to complete penetration testing that will simulate tactics that may be used by attackers.

31 The Act will provide for a range of penalties should providers contravene their legal duties. These penalties consist of fines to a maximum of 10% of turnover or a daily penalty of £100,000 for continuing offences. Equally there will be increased penalties for security related information offences of up to £50,000 per day or a maximum of £10 million.

32 To ensure the Government can oversee the regime, Ofcom will be able to share information with the Government. For example, it can notify the Government about security incidents or the risks of security incidents. The Act also makes provisions for Ofcom to report on telecoms providers' security to the Secretary of State. These reports will set out the extent to which providers are complying with new security obligations and are acting in accordance with the code of practice, as well as any action that Ofcom has taken in response to security compromises. Telecoms security will also be included in Ofcom's periodic infrastructure report.

National Security Powers

33 Telecoms security risks can to a large extent be managed and mitigated through technical measures (detailed in the security framework and the code of practice as set out above). However, the Government considers that some risks relating to the use of high risk vendors' goods, services and facilities are not able to be mitigated effectively solely through the requirements that will be imposed as part of the new telecoms security framework. Further measures are needed to enable the Government to manage the risks posed by those vendors. Such risks may arise from technical deficiencies or considerations relating to the ownership and operating location of the vendor.

34 This Act will introduce new powers to enable the Secretary of State to designate specific vendors for the purposes of issuing designated vendor directions to public communications providers (see definition in Annex A). The designated vendor directions will place restrictions on the public communications provider's use of the goods, services or facilities supplied by designated vendors. The restrictions that may be imposed include requirements that prohibit or restrict providers' use of designated vendors' equipment.

35 Designations and directions may only be made in the interests of national security. When considering whether to designate a vendor, the Secretary of State will take into account a range of factors, including:

- the strategic position or scale of the vendor in UK networks;

- the strategic position or scale of the vendor in other telecoms networks, particularly if the vendor is new to the UK market;
- the quality and transparency of the vendor's engineering practices and cyber security controls;
- the vendor's resilience both in technical terms and in relation to the continuity of supply to UK operators;
- security laws in the jurisdiction where the vendor is based and the risk of external direction that conflicts with the interests of national security;
- the relationship between the vendor and the vendor's domestic state apparatus;
- the availability of offensive cyber capability by that domestic state apparatus, or associated actors, that might affect the national security of any country or territory.

36 The Act will make it a duty for public communications providers to comply with any requirements specified in a designated vendor direction that follows designation, and will enable appropriate sanctions to be imposed for non-compliance. The Secretary of State will be responsible for taking forward any enforcement action as necessary, drawing upon information provided by Ofcom, who can be tasked under the Act's provisions to gather information on telecoms providers' use of designated vendors' goods, services and facilities in relation to their compliance with requirements imposed in a designated vendor direction.

37 The Act will create a power for the Secretary of State to require information from public communications providers about their current or planned use of vendors' goods, services or facilities, or about the future development of their networks or services. This power can also be used to gather information about goods, services or facilities that vendors propose to supply. The power will be used to ensure the Secretary of State is informed about the demand and supply side of the telecoms market, enabling relevant security assessments to be made.

38 The Act will also enable the Secretary of State to require providers to prepare and provide a plan to the Secretary of State and Ofcom setting out how they intend to meet any requirements specified in a direction.

Legal background

39 The existing legal framework for the regulation of telecommunications is primarily set out in Part 2 of the 2003 Act. This implemented the European common regulatory framework for electronic communications, which comprised a set of four EU directives (the Framework Directive (2002/21/EC), the Access Directive (2002/19/EC), the Authorisation Directive (2002/20/EC) and the Universal Service Directive (2002/22/EC)).

40 Those directives are replaced by Directive (EU) 2018/1972 establishing the European Electronic Communications Code ("the EECC Directive"). The Electronic Communications and Wireless Telegraphy (Amendment) (European Electronic Communications Code and EU Exit) Regulations 2020/1419, which implement the EECC Directive, have been approved by both Houses of Parliament.

41 The Act replaces the existing legal framework relating to the security of public electronic communications networks and services under sections 105A to 105D of the 2003 Act. These

sections were inserted in 2011 to implement Articles 13a and 13b of the Framework Directive (as amended by Directive 2009/140/EC).

42 Other related legislation includes the Privacy and Electronic Communications (EC Directive) Regulations 2003/2426 (as amended) which contain certain provisions relating to the security of public electronic communications services insofar as relevant to the processing of personal data in the electronic communications sector.

43 The Network and Information Systems Regulations 2018/506 (as amended) make provision about the security of 'network and information systems' on which 'essential services' in various critical sectors depend. The regulations implemented Directive (EU) 2016/1148, which was itself modelled on Articles 13a and 13b of the Framework Directive. Providers of public electronic communications networks and public electronic communications services therefore fall outside the scope of these regulations, but Ofcom regulates the 'digital infrastructure' sector which consists of domain name system (DNS) services, domain name registries and internet exchange points.

Territorial extent and application

44 The Act extends and applies to the whole of the UK.

45 Telecommunications and wireless telegraphy are reserved matters under each of the devolution settlements: see paragraph C10 in Part II of Schedule 5 to the Scotland Act 1998, paragraph 83 in section C9 of Part 2 of Schedule 7A to the Government of Wales Act 2006, and paragraph 29 of Schedule 3 to the Northern Ireland Act 1998.

46 National security is also a reserved or excepted matter under each of the devolution settlements: see paragraph B8 of Part II of Schedule 5 to the Scotland Act 1998, paragraph 32 in section B3 of Part 2 of Schedule 7A to the Government of Wales Act 2006, and paragraph 17 of Schedule 2 to the Northern Ireland Act 1998.

Commentary on provisions of Act

Section 1: Duty to take security measures

47 This section places a new duty on providers to take security measures. To complement this overarching duty, the section allows the Secretary of State to impose more specific security duties on providers by regulations.

48 The section replaces sections 105A to 105D of the 2003 Act with new sections 105A and 105B.

Section 105A: Duty to take security measures

49 Subsection (1) requires providers to take steps to identify and reduce the risks of security compromises occurring and prepare for the occurrence of security compromises.

50 Security measures for the purpose of identifying the risk of security compromises would include the provider carrying out a risk assessment in relation to its network or service.

51 Security measures for the purpose of reducing the risk of security compromises would include measures taken in the design of the network or service (such as segregation of the most sensitive controls from the rest of the network).

52 Security measures for the purpose of preparing for the occurrence of security compromises would include measures such as retaining copies of information that would enable the running of functions that are most critical to a network or service in the event that these were compromised. Other measures may address the secure operation of the network or service. This could take the form of having procedures in place to monitor the network for abnormalities so that security compromises can be identified and remedied as quickly as possible.

53 Subsection (2) defines "security compromise". The definition is broad and includes (among other things) anything that compromises the availability, performance or functionality of the network or service, or that compromises the confidentiality of the signals conveyed by means of the network or service. It also covers any unauthorised access to, interference with or exploitation of the network or service. Exploitation would include the misuse of a network or service's functionality in unintended or unauthorised ways or for unintended or unauthorised purposes (for instance by using functionality that supports the provision of interpersonal communications services for other purposes, such as espionage).

54 Subsection (3) provides that the definition of security compromises does not include anything that occurs as the result of certain kinds of conduct. This includes, for example, conduct that is required or authorised under enactments such as the Investigatory Powers Act 2016, ensuring that the Act does not adversely affect lawful activity carried out by law enforcement authorities or by the intelligence services which could otherwise fall within the definition of security compromise.

55 Subsection (4) lists enactments for the purpose of subsection (3), and includes enactment that makes provision which is in the interests of national security, has effect for the purpose of preventing or detecting crime or preventing disorder, or makes provision which is in the interest of the economic well-being of the UK as far as those interests are relevant to national security.

Section 105B: Duty to take specified security measures

56 Subsection (1) provides the Secretary of State with the power to make regulations which require providers to take specified security measures.

57 Subsection (2) provides that such measures may only be specified in regulations if the Secretary of State considers that they would be appropriate and proportionate for one of the purposes identified in subsection 105A(1).

Section 2: Duty to take measures in response to security compromises

58 This section requires providers to take measures in response to security compromises, as defined in new section 105A. To complement the overarching duty, the section allows the Secretary of State to impose specific security duties on providers by regulations.

59 The section inserts new sections 105C and 105D into the 2003 Act.

Section 105C: Duty to take measures in response to security compromises

60 Subsection (2) places a duty on providers to take measures to prevent adverse effects arising from a security compromise that has occurred. This is not limited to adverse effects on the network or service itself. Where the security compromise has an adverse effect on the network or service, subsection (3) requires the provider to take measures to remedy or mitigate that effect.

Section 105D: Duty to take specified security measures in response to security compromises

61 Subsection (1) provides the Secretary of State with the power to make regulations which require providers to take specified measures in response to a specified security compromise.

62 Subsection (2) explains that providers can only be required to take measures that the Secretary of State considers are appropriate and proportionate to prevent adverse effects arising from the specified security compromise.

63 Subsection (3) provides the Secretary of State with the power to make regulations which require providers to take specified measures where a security compromise has a specified adverse effect on the network or service.

64 Subsection (4) explains that providers can only be required to take measures that the Secretary of State considers are appropriate and proportionate ways to remedy or mitigate the specified adverse effect.

Section 3: Codes of practice about security measures

65 This section gives the Secretary of State the power to issue a code of practice providing guidance to providers on measures to take in order to meet the new security duties within the Act. It includes provisions relating to the issuing, revision and re-issuing, withdrawal and effects of a code of practice. It also includes a duty on providers to explain any failure to comply with the measures in a code of practice, when directed to do so by Ofcom.

66 The section inserts new sections 105E to 105I into the 2003 Act.

67 The issuing of the code of practice is subject to the negative resolution procedure. Parliament are provided with a 40-day period in which they are able to choose not to approve the issuing of the draft code.

Section 105E: Codes of practice about security measures etc

68 Section 105E allows the Secretary of State to issue, revise and re-issue or withdraw a code of practice which gives guidance on the measures to be taken by providers under sections 105A to 105D.

Section 105F: Issuing codes of practice about security measures

69 Subsection (1) sets out what the Secretary of State must do before issuing a code of practice. It explains that the Secretary of State:

- must publish a draft of the code or the revisions of the code;
- must consult about the draft with Ofcom, providers to whom the draft would apply, and other persons as appropriate; and
- may make alterations to the draft after consultation if appropriate.

70 Subsection (2) requires the Secretary of State to lay a draft of the code before Parliament. Subsections (3), (4) and (5) set out the ability of Parliament to scrutinise a draft code within a 40-day period, during which it can resolve not to approve a code of practice. If no resolution is made the Secretary of State may issue the code of practice and publish it. Subsections (6) and (7) set out commencement dates for different purposes. Subsections (8) and (9) relate to the definition of the 40-day scrutiny period.

Section 105G: Withdrawing codes of practice about security measures

71 Section 105G sets out what the Secretary of State must do before and after withdrawing a code of practice.

72 Subsection (1) states that before withdrawing a code of practice, the Secretary of State must publish notice of the proposal and must consult about the proposal with Ofcom, providers to whom the draft would apply, and other persons as appropriate.

73 Subsection (2) states that where the Secretary of State withdraws a code of practice they must publish notice of the withdrawal and lay the notice before Parliament.

74 Subsections (3) and (4) set out the withdrawal arrangements, including the ability of a code to specify different withdrawal dates for different purposes.

Section 105H: Effects of codes of practice about security measures

75 Subsection (1) makes clear that codes are guidance and that a failure to act in accordance with their provision does not of itself make a provider liable to legal proceedings. When determining any question in legal proceedings, the court must take into account any provisions of the code which were in force at the time and appear relevant (subsection (2)).

76 Subsection (3) provides that Ofcom must take a code provision into account in determining any question while carrying out its relevant functions, where such provision is in force at the time and appears relevant. The list of relevant functions is set out at subsection (4).

Section 105I: Duty to explain failure to act in accordance with code of practice

77 Section 105I allows Ofcom to notify a provider where Ofcom deems it is failing or has failed to act in accordance with a code. The notification must set out how the provider is suspected to have contravened the code and direct the provider to give a statement in response. In its statement, the provider must either confirm or deny Ofcom's suspicions and give a supporting explanation.

Section 4: Informing others of security compromises

78 This section places new duties on providers to report security incidents to Ofcom and inform the users of telecoms networks and services of the associated risks. The section is designed to transpose the intent of the security aspects of the European Electronic Communications Code (EECC).

79 The section inserts new sections 105J to 105L into the 2003 Act.

Section 105J: Duty to inform users of risk of security compromise

80 Section 105J places a duty on providers to take reasonable steps to inform users about security compromises or where there is a significant risk of a security compromise occurring and the user may be adversely affected as a result.

81 The purpose of this section is to allow providers to inform users who may be adversely affected by the security compromise, and to give the user the information they would need to take steps to prevent, remedy or mitigate the adverse effect that the security compromise would have on them. An example of the type of steps that a user may take could be changing their password.

82 Specifically, the provider must inform the user about the existence of the risk, the nature of the security compromise, the steps which could reasonably be taken by users 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 (subsection (3)).

83 By 'reasonable and proportionate' this section intends that reasonable steps should be taken by providers which are proportionate to the size and impact of compromise risk, both in relation to the way the information is shared, and the time at which the information is provided. For example, in some circumstances, if a risk can be mitigated quickly it may be more reasonable for short term mitigation measures to be put in place before users are informed, if this provides better protection to the network or service and ultimately the user.

Section 105K: Duty to inform Ofcom of security compromise

84 The intention of Section 105K is to increase the reporting of security incidents by providers to Ofcom. This will give Ofcom a better understanding of the security risks across the telecoms industry.

85 Subsection (1) places a duty on providers to inform Ofcom as soon as reasonably possible of any security compromise that:

- has a significant effect on the network or service; or
- involves unauthorised access to or interference with the network or service so that a person is put in a position to bring about a security compromise that could significantly affect the network or service.

86 The wording of subsection (1)(b) is designed to ensure the reporting of 'pre-positioning' attacks that do not at the time of the attack affect the network or service, but do allow access to a network that could result in future security compromises.

87 Subsection (2) states that in determining whether the effect of a security compromise is, or could be, significant a number of factors should be taken into account, such as the number of people who are, or might be, affected.

Section 105L: Powers of Ofcom to inform others of security compromise

88 Section 105L applies where Ofcom considers that there is a risk of a security compromise occurring or a security compromise has occurred. The circumstances in which Ofcom must inform the Secretary of State of the above are set out in subsection (2).

89 In this situation, Ofcom must inform the Secretary of State of the above where the security compromise could (or already has had) specified serious consequences, such as a serious threat to national security (subsection (2)).

90 Ofcom may still inform the Secretary of State that there is a risk of a security compromise occurring or a security compromise has occurred even where there is no duty to do so (subsection (3)).

91 Subsection (4) identifies additional groups or organisations which Ofcom may inform about security compromises, namely network or service users, providers, overseas regulators and the European Union Agency for Cybersecurity.

92 Subsection (5) allows Ofcom to inform network or service users of measures that they can take to prevent, remedy and mitigate the adverse effects of the security compromises.

93 Subsection (6) allows Ofcom to direct providers to take steps to inform users (or previous users) of the risk of (or occurrence of) a security compromise and measures that they can take to prevent, remedy and mitigate the adverse effects.

94 Subsection (7) allows Ofcom, if they consider it to be in the public interest, to inform the public (either directly or via a provider) about the risk of (or occurrence of) the security compromises and the protective measures that may be taken.

95 Subsection (8) places a duty on providers to comply with a direction given under this section within the reasonable period specified in the direction.

96 Subsection (9) defines "overseas regulator" (as used in 105K(4)) as any person who under the law of a country outside the United Kingdom has functions that correspond to the functions of Ofcom in relation to networks and services.

Other provisions

97 Subsection (3) of section 4 provides for an amendment of section 393(6) of the 2003 Act so that nothing in that section prevents the disclosure of information under 105L.

Section 5: General duty of Ofcom to ensure compliance with security duties

98 This section places a duty on Ofcom to ensure that providers comply with their security duties under sections 105A, 105B, 105C, 105D, 105J and 105K.

99 The section inserts new section 105M into the 2003 Act.

Section 105M: General duty of Ofcom to ensure compliance with security duties

100 Section 105M requires Ofcom to seek to ensure that providers comply with the security duties imposed on them by sections 105A, 105B, 105C, 105D, 105J and 105K.

Section 6: Powers of Ofcom to assess compliance with security duties

101 This section sets out the powers of Ofcom to assess providers' compliance with their security duties. It permits Ofcom to issue assessment notices that require providers to do various things, such as carry out tests and permit an authorised person to enter their premises. The use of assessment notices will be a key means of collecting data for assessing compliance with the security duties. The costs of carrying out an assessment will be borne by the provider.

102 The section inserts new sections 105N to 105R into the 2003 Act.

Section 105N: Power of Ofcom to assess compliance with security duties

103 Subsection (1) 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, 105B, 105C, 105D, 105J and 105K.

104 Subsection (2) imposes a duty on providers to cooperate with an assessment. This would include not doing anything to disrupt an assessment, such as destroying documents to which access is sought or interfering with testing required by an assessment notice. The costs of an assessment will be borne by the provider.

Section 105O: Power of Ofcom to give assessment notices

105 Subsection (2) 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. Examples include carrying out specified tests, arranging for another person to carry out specified tests, and making people available for interview. It also includes permitting authorised persons to enter specified premises for various purposes, such as to observe any relevant operations taking place. The specified premises cannot be domestic premises (subsection (5)).

106 Subsection (3) provides that the tests required by an assessment notice can include tests of premises and/or persons involved in the provision of the network or service.

107 Subsection (4) provides that 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. This includes 'penetration testing' and 'red teaming exercises'.

108 Subsection (6) ensures that an assessment notice may not require the provider to take actions that would violate legal privilege.

109 Subsection (7) requires the assessment notice to set out the times at which each duty in the notice must be complied with. An assessment notice cannot require a provider to do anything before the end of the period within which the notice can be appealed, namely two months from the date of the notice in accordance with the Competition Appeal Tribunal Rules 2015. If a provider appeals an assessment notice it does not need to comply with the notice until the appeal is resolved.

110 Subsection (10) requires an assessment notice to provide information about the consequences of a failure to comply with it and the right of appeal.

111 Subsection (11) permits Ofcom to cancel a notice or make it less onerous by giving notice to the provider.

Section 105P: Assessment notices: urgency statements

112 Section 105P allows Ofcom to issue an assessment notice which requires that the provider must comply with a duty urgently. Such a notice must explain why this is the case and inform the provider of the right to make an application under section 105Q.

113 Subsection (2) sets out the effect of an urgency statement. The usual rules regarding the timeframe for complying with a duty and how this may be affected by an appeal, as set out under subsections 105O(8) and (9), do not apply to duties which must be complied with urgently. Instead, the relevant rules are set out at subsections 105P(3) and (4).

114 Subsections (3) provides that an assessment notice cannot require the provider to comply with an urgent duty at a time that falls (or a period that begins) within 14 days of the notice being issued.

115 Subsection (4) states that, where an urgent duty is a duty which involves permitting an authorised person to enter specified premises or concerns the provision of documents (i.e. duties under subsection (2)(d) to (k)) and the obligation to comply with the duty is appealed within 14 days of the notice being issued, the provider does not need to comply with the duty until the appeal is resolved.

Section 105Q: Assessment notices: applications in respect of urgency statements

116 Section (2) provides that, where a provider is obliged to comply with a duty urgently, it may apply to the court (i.e. the High Court or Court of Session) for an order that the duty 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.

Section 105R: Assessment notices: information about entering premises

117 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.

Other provisions

118 Subsection (3) of section 6 amends section 135 of the 2003 Act to add the act of carrying out an assessment under this section as a particular purpose for which Ofcom may require information.

119 Subsection (4) of section 6 amends Schedule 8 of the 2003 Act so that a decision that a duty must be complied with urgently (pursuant to section 105P(1)(b)) is not subject to appeal to the Competition Appeals Tribunal.

Section 7: Powers of Ofcom to enforce compliance with security duties

120 This section sets out the powers of Ofcom to enforce the security duties. This includes setting out penalties for non-compliance.

121 The section inserts new sections 105S to 105V into the 2003 Act.

Section 105S: Enforcement of security duties

122 Subsection (1) states that sections 96A to 100, 102 and 103 of the 2003 Act, which apply to contraventions of conditions set under section 45, also apply in relation to a contravention of a security duty. In summary:

- Section 96A allows Ofcom to issue a notification to a person they reasonably consider to have contravened or be contravening a condition set under section 45. Subsection 96A(2) lists the points that a notification must specify.
- Section 96B sets out the requirements for penalties which may be included in a notification under section 96A, including the maximum amount of a daily penalty (subsection (5)).
- Section 96C provides for the enforcement of notifications given under section 96A.
- Section 97 sets out the amount of a penalty given under section 96A. The maximum amount of a penalty (other than a penalty for a continuing contravention) is 10 percent of the turnover of the person's business (subsection (1)).
- Section 98 gives Ofcom the power to deal with urgent cases where they are entitled to give a notification under section 96A. This includes the power to suspend or restrict the contravening provider's entitlement to provide networks or services (subsection 98(4)).

- Section 99 sets out the process which must be followed by Ofcom after they have given a direction under subsection 98(4).
- Section 100 concerns the suspension of service provision for contravention of conditions.
- Section 102 sets out the procedure for directions under section 100.
- Section 103 concerns the enforcement of decisions under sections 98 and 100.

123 Subsection (2) provides that this section is subject to section 105T, which concerns the enforcement of security duties and the amount of penalties.

124 Subsection (3) explains that "security duty" means a duty imposed by sections 105A, 105B, 105C, 105D, 105I, 105J, 105K, 105L(6), (7)(c) and (8), 105N(2)(a) and 105O.

Section 105T: Enforcement of security duties: amount of penalties

125 This section sets out the penalties for continuing non-compliance with security duties in the Act, and gives the Secretary of State a regulation making power to amend those penalties.

126 Subsection (1) states that the penalty for continuing non-compliance with a security duty, other than the duty under 105I, is a daily penalty of up to £100,000.

127 Subsection (2) states that the penalty for continuing non-compliance with the security duty imposed by 105I is a daily penalty of up to £50,000.

128 Subsection (3) states that the maximum penalty for a contravention of the security duty imposed by 105I (not including continuing contraventions) is £10 million.

129 Subsection (4) gives the Secretary of State a power to amend the amounts set out in subsections (1), (2), and (3).

130 Subsection (5) states that regulations made under this section must be laid before Parliament in draft and approved by a resolution in each House.

Section 105U: Enforcement of security duties: proposal for interim steps

131 Section 105U allows Ofcom to propose interim steps to a provider pending the commencement or completion of enforcement action described under section 105S.

132 Subsection (1) sets out the conditions which must be met before Ofcom may propose interim steps to a provider, namely:

- 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 has not yet commenced enforcement action (under section 96A) or 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 occurring;
- it is reasonable to require the provider to take interim steps given the seriousness or likely seriousness of the security compromise.

133 Where the above conditions are met, subsection (2) allows Ofcom to give a notification to the provider setting out, amongst other things, the interim steps which Ofcom think the provider should take pending the completion of enforcement action.

134 Subsection (3) provides that commencement by Ofcom of enforcement action means the giving of a notification under section 96A, and completion of enforcement action means the taking of action under section 96C(2)(a) or (b).

135 Subsection (4) sets out the nature of the "interim steps" which may be required of a provider, such as preventing or limiting the adverse effects of a security compromise.

Section 105V: Enforcement of security duties: direction to take interim steps

136 Section 105V provides that, after Ofcom has given a provider a notification under section 105U, it must allow the provider an opportunity to make representations in response. Ofcom may only direct the provider to take the interim steps once the period allowed for representations is over (subsection (2)).

137 Subsection (3) states that Ofcom may only direct a provider to take interim steps if they are satisfied that:

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

138 Subsection (4) states that a direction to take interim steps must include a statement of reasons.

139 Subsection (5) states that a direction must set out the time period within which each interim step must be taken.

140 Subsection (6) states that a direction cannot require a provider to take interim steps after the completion of enforcement action by Ofcom.

141 Subsection (7) requires Ofcom to commence or complete enforcement action as soon as reasonably practicable after a direction to take interim steps has been given.

142 Subsection (8) states that a direction may at any time be revoked by Ofcom or varied to make it less onerous.

143 Subsection (9) states that a provider must comply with a direction given to them to take interim steps under subsection (2)(a).

144 Subsection (10) states that the duty to comply with directions under this section is enforceable in civil proceedings by Ofcom.

Section 8: Civil liability for contravention of security duties

145 This section makes provision for civil liability for contravention of security duties.

146 The section inserts new section 105W into the 2003 Act.

Section 105W: Civil liability for breach of security duty

147 Section 105W makes the contravention of specified security duties actionable in civil proceedings where the breach of the duty causes loss or damage.

148 Subsection (1) provides that the security duties placed on providers under sections 105A, 105B, 105C, 105D and 105J are owed to every person who may be affected by a contravention.

149 Subsection (3) provides that a person who suffers loss or damage as the result of a breach of the above security duties may bring legal proceedings in respect of the breach. Subsection (5) provides that it is a defence for a provider to show that they took all reasonable steps and exercised all due diligence to avoid contravening the duty.

150 Subsection (4) provides that a person may also bring legal proceedings where they have suffered loss or damage as the result of an act which induces a breach of duty or interferes with its performance. The act must be done with the intention that it will cause the person to suffer loss.

151 Subsection (6) provides that Ofcom must consent to the bringing of proceedings under this section, which may be subject to conditions relating to the conduct of proceedings (subsection 7).

Section 9: Relationship between security duties and certain other duties etc

152 This section addresses the relationship between the security duties created by the Act, and duties under other legislation and certain other conduct.

Section 105X: Relationship between security duties and certain other duties etc

153 Subsection (1) provides that a security duty (as defined in subsection (2)) does not apply in so far as compliance with the duty would result in a failure by the provider to comply with a duty or prohibition imposed by an enactment mentioned in 105A(4) or prevent the provider from undertaking certain other conduct. This includes, for instance, assisting the police in giving effect to a warrant or authorisation that has been issued under an enactment listed in 105A(4).

Section 10: Statement of policy on ensuring compliance with security duties

154 This section requires Ofcom to publish a statement of policy explaining how they will ensure compliance with the security duties.

155 The section inserts new section 105Y into the 2003 Act.

Section 105Y: Statement of policy on ensuring compliance with security duties

156 Subsection (1) requires Ofcom to prepare and publish a statement setting out their general policy regarding how they will exercise their various powers to ensure that providers comply with their security duties (see sections 105I and 105M to 105V).

157 Subsection (2) permits Ofcom to revise the statement as they think fit.

158 Subsection (3) requires Ofcom to publish their policy statement (and any revisions of the statement) in a manner which they consider will bring it to the attention of those who are likely to be affected by it.

159 Subsection (4) requires Ofcom to have regard to their statement when exercising their functions under sections 105I and 105M to 105V.

Other provisions

160 Subsection (3) of section 10 amends Schedule 8 of the 2003 Act to ensure that Ofcom's decisions relating to the making or revising of a statement under this section are not subject to appeal by tribunal.

Section 11: Reporting on matters related to security

161 This section makes provision about reporting by Ofcom on matters relating to security, including a duty to provide an annual security report to the Secretary of State.

162 The section inserts new section 105Z into the 2003 Act.

Section 105Z: Ofcom reports on security

163 Subsection (1) requires Ofcom to send periodic security reports to the Secretary of State as soon as practicable after the end of each reporting period. The reporting period is two years from the day on which the section comes into force and each successive twelve-month period after this date.

164 Subsections (2) and (3) provide that a security report must contain information and advice which will assist the Secretary of State to formulate policy regarding the security of public electronic communication networks and services.

165 Subsection (4) sets out matters which must be included in a security report, such as information about the extent to which providers have complied with security duties during the reporting period.

166 Subsection (5) states that the security report must not include personal data (i.e. any information relating to an identified or identifiable living individual).

167 Subsection (6) allows the Secretary of State to publish a security report or disclose it to any person or body discharging functions of a public nature in order to enable or assist the discharge of those functions.

168 Subsections (7) and (8) requires the Secretary of State to consider the need to keep confidential matters relating to the affairs of a particular body, the disclosure of which might seriously or prejudicially affect the interests of that body before publishing or disclosing a security report.

Other provisions

169 Subsection (3) of section 11 amends section 134B of the 2003 Act so that Ofcom's reports on infrastructure under sections 134A and 134AA should deal with the extent to which providers are complying with their duties under sections 105A, 105B, 105C and 105D.

170 Subsection (4) of section 11 allows Ofcom to require information from a person under section 135 of the 2003 Act for the purpose of preparing a report under section 105Z.

171 Subsection (5) of section 11 ensures that nothing in section 393 prevents the publication or disclosure of a report under subsection 105Z(6).

172 Subsection (6) of section 11 amends Schedule 8 of the 2003 Act to ensure that Ofcom's decisions relating to the making of a report under this section are not subject to appeal to the Competition Appeals Tribunal.

Section 12: Powers to require and share information related to security

173 This section sets out Ofcom's powers to require and share information concerning the security of public electronic communications networks and services.

174 Subsection (2) ensures that section 24B(2), which limits Ofcom's ability to provide certain information to the Secretary of State, does not prevent Ofcom from providing information which they consider may assist the Secretary of State with the formulation of policy in relation to the security of public electronic communications networks and services.

175 Subsection (3) amends section 135 so that:

- Ofcom can require information from a person for the purpose of assessing the risk of a security compromise occurring (subsection (3)(a)).
- The information which Ofcom can require from a person can include information concerning future developments of a public electronic communications network or service that could have an impact on the security of the network or service (subsection (3)(b)).
- Ofcom can require a person to take actions to facilitate the provision of security information, such as obtaining and retaining such information (subsection (3)(c)). Security information is defined as information which Ofcom considers necessary for the purpose of carrying out their functions under sections 105M to 105Z (subsection (3)(d)).

176 Subsection (4) amends section 137 of the 2003 Act to state that Ofcom must provide reasons for putting a requirement on providers under 135(3C).

Section 13: Appeals against security decisions of Ofcom

177 This section concerns the disposal of appeals against certain security-related decisions made by Ofcom.

178 This section amends section 194A of the 2003 Act, which concerns the disposal of appeals under section 192 by the Competition Appeal Tribunal. It inserts new subsections (2A) and (2B), which provide that when deciding an appeal against certain security-related decisions made by Ofcom, the Tribunal is to apply judicial review principles without taking any special account of the merits of the case. The effect of this is that, in such appeals, the Tribunal should not adopt a modified approach in light of provisions in EU law (specifically, Article 31 of Directive (EU) 2018/1972 which provide for "*the merits of the case*" to be "*duly taken in account*").

Section 14: Reviews of sections 1 to 13

179 This section states that the Secretary of States must review sections 1 to 13 at least every five years.

180 Subsection (1) requires the Secretary of State to review the impact and effectiveness of sections 1 to 13.

181 Subsection (2) requires the Secretary of State to publish a report of each review and lay it before Parliament.

182 Subsection (3) requires the reports to be published at least every five years.

183 Subsection (4) states that the first report must be published within five years of the day on which the Act is passed.

Section 15: Designated vendor directions

184 This section gives the Secretary of State the power to give a direction to a public communications provider ("provider") that imposes requirements on the provider's use of goods, services or facilities supplied, provided or made available by a designated vendor. The sections in this section set out when a direction may be given, the process to be followed, the types of requirements that a direction may impose and how such requirements may be varied or revoked.

185 The section inserts new sections 105Z1 to 105Z7 into the 2003 Act.

Section 105Z1: Designated vendor directions

186 This section allows the Secretary of State to give a direction to a provider which imposes requirements on their use of goods, services or facilities supplied by a specified "designated vendor" as designated under section 105Z8.

187 Subsection (2) provides that the Secretary of State may only give a designated vendor direction if the Secretary of State considers it to be necessary in the interests of national security and that the requirements imposed by the direction are proportionate.

188 Subsection (3) states that requirements imposed by a direction may only apply with respect to the use of goods, services or facilities provided by a designated vendor in connection with certain purposes (as set out in subsection (4)), such as providing a public electronic communications network or service. The goods, services and facilities need only be used in connection with, rather than be necessary for, the provision of a public electronic communications network, service, or associated facility or the enabling of persons to make use of such networks or services, in order for requirements to be applied.

189 Subsection (5) requires a direction to specify which providers it applies to, the time at which it comes into force and the reasons for which it was given.

190 Subsection (6) states that the direction does not need to give reasons where the Secretary of State considers that doing so would be contrary to the interests of national security.

191 Subsection (7) imposes a duty on a provider in receipt of a direction to comply with the direction.

Section 105Z2: Further provision about requirements

192 This section provides further detail on the types of requirements that may be imposed on a provider's use of goods, services or facilities supplied by a designated vendor.

193 Subsection (2) outlines the types of requirements that may be imposed by a direction. Requirements may include, among other things, requirements to prohibit or restrict use of goods, services, or facilities supplied, provided, or made available by a designated vendor, and requirements to remove, disable and modify goods, services or facilities supplied, provided or made available by a designated vendor.

194 Subsections (3), (4), (5) and (6) further expand on the scope and flexibility of the requirements that may be imposed by a direction:

- For example, a requirement in a direction may refer to the source of the goods, services or facilities, the time at which goods, service or facilities were developed or produced, or the time at which goods, services or facilities were procured, supplied, provided or made available (subsection (4)(a)(b) and (c)).
- A requirement may be imposed which only applies in certain circumstances (subsection (5)).
- A designated vendor direction may provide for exceptions to a requirement (subsection (6)).

195 Subsections (7) and (8) state that a requirement in a direction must specify the period for compliance and that this period must be reasonable.

Section 105Z3: Consultation about designated vendor directions

196 This section sets out the requirement to consult before a designated vendor direction is given.

197 Subsection (1) requires the Secretary of State to consult providers and relevant vendors before giving a direction where this is reasonably practicable. This does not apply where such consultation would be contrary to the interests of national security (subsection (2)).

Section 105Z4: Notice of designated vendor directions

198 This section sets out when a designated vendor direction should also be sent to the designated vendor.

199 Subsection (1) requires a copy of a direction to be sent to the designated vendor specified in the direction where this is reasonably practicable. This does not apply where such actions would be contrary to the interests of national security (subsection (2)).

200 Subsection (3) allows the Secretary of State to exclude from a copy of a direction anything which might prejudice to an unreasonable degree any person's commercial interests or be contrary to the interests of national security if disclosed.

Section 105Z5: Variation and revocation of designated vendor directions

201 This section sets out when and how the Secretary of State may vary or revoke a direction.

202 Subsection (1) states the Secretary of State must periodically review directions.

203 Subsection (2) allows the Secretary of State to vary or revoke a direction or part of a direction.

204 Subsection (3) provides that a direction may only be varied if it is necessary in the interests of national security and the varied requirements are proportionate.

205 Subsection (4) requires the Secretary of State to consult the provider and designated vendor where reasonably practicable before varying a direction. This does not apply where such consultation would be contrary to the interests of national security (subsection (5)).

Section 105Z6: Notice of variation and revocation of designated vendor directions

206 This section sets out the notice requirements where the Secretary of State seeks to vary and/or revoke a designated vendor direction.

207 Subsection (1) requires the Secretary of State to notify providers when a direction is varied.

208 Subsection (2) requires the notice to specify how the direction is varied, the time at which the varied requirements come into force and the reasons for the variation.

209 Subsection (3) provides that reasons do not need to be given where the Secretary of State considers that doing so would be contrary to the interests of national security.

210 Subsection (4) states that the Secretary of State must send a copy of the notice to the relevant designated vendor where this is reasonably practicable. This does not apply where doing so would be contrary to the interests of national security (subsection (5)).

211 Subsection (6) allows the Secretary of State to exclude from a copy of a notice anything which might prejudice to an unreasonable degree any person's commercial interests or be contrary to the interests of national security if disclosed.

212 Subsections (7) to (11) replicate in part the subsections above but in relation to notices of revocation rather than variation. Notice of a revocation must be given to providers and designated vendors who were subject to the direction as it had effect before the revocation, providing this would not be contrary to interests of national security.

Section 105Z7: Designated vendor directions: plans for compliance

213 This section gives the Secretary of State the power to require providers to prepare and provide a plan to the Secretary of State setting out the steps the provider intends to take to comply with a designated vendor direction. The Secretary of State may also require this plan to be provided to Ofcom.

Section 16: Designation notices

214 This section gives the Secretary of State the power to designate vendors for the purposes of issuing a designated vendor direction. The sections in this section outline the factors the Secretary of State will consider before issuing a designation notice, describe the process that will be followed and describe the way in which designation notices may be amended or revoked.

215 The section inserts new sections 105Z8 to 105Z10 into the 2003 Act.

Section 105Z8: Designation notices

216 This section sets out the Secretary of State's power to designate vendors for the purposes of issuing a designated vendor direction. It lists the primary factors that may be taken into account when considering whether or not to designate a vendor.

217 Subsections (1) to (3) allow the Secretary of State to issue a notice which designates a person (or persons) for the purposes of a designated vendor direction (see sections 105Z1 to 105Z7) providing that the Secretary of State considers it is necessary in the interests of national security.

218 Subsection (4) lists the principal matters which the Secretary of State may have regard to when considering whether to designate a person under subsection (1). There are a wide range of matters, which include the nature of the goods, services or facilities supplied, the reliability of such products, the identity of the persons who own or control the person being considered for designation, and the country or territory in which the registered office or any place of business of the person being considered for designation is located.

219 Subsection (5) states that a designation notice must specify the reasons for designation. This does not apply where the Secretary of State considers that it would be contrary to the interests of national security (subsection (6)).

Section 105Z9: Further provision about designation notices

220 This section sets out the requirement to consult persons before and notify them after designation takes place under section 105Z8.

221 Subsection (1) requires the Secretary of State to consult the persons proposed to be designated where reasonably practicable. This does not apply where the Secretary of State considers that it would be contrary to the interests of national security (subsection (2)).

222 Subsection (3) requires the Secretary of State to serve a designation notice on the designated person(s) where this is reasonably practicable.

Section 105Z10: Variation and revocation of designation notices

223 This section sets out the Secretary of State's power to vary or revoke a designation notice given under section 105Z8 and the associated requirements for consultation and notification.

224 Subsection (1) requires the Secretary of State to periodically review designation notices.

225 Subsection (2) allows the Secretary of State to vary or revoke a designation notice, although a notice may only be varied if it is in the interests of national security (subsection (3)). Before

varying a notice, the Secretary of State must, where reasonably practicable, consult the person who is proposed to be designated in the varied notice (subsection (4)), unless this would be contrary to the interests of national security (subsection (5)).

226 Subsection (6) requires the Secretary of State, where reasonably practicable, to notify persons about a variation if they are designated in the varied notice or were designated before the variation.

227 Subsection (7) requires the notice of variation to state how the designation is varied, the time when the variation, or each of them, comes into force and the reasons for the variation. Reasons do not need to be provided where this would be contrary to the interests of national security (subsection (8)).

228 Subsections (9) and (10) replicate in part the provisions relating to giving notice of variation and what the notice must specify, but for a notice of revocation rather than variation.

Section 17: Laying before Parliament

229 This section requires the Secretary of State to lay before Parliament copies of documents connected with the designation of vendors and designated vendor directions produced under sections 105Z1 to 105Z10.

230 The section inserts new section 105Z11 into the 2003 Act.

Section 105Z11: Laying before Parliament

231 Subsection (1) requires the Secretary of State to lay before Parliament copies of designated vendor directions and designation notices, as well as notices of variation and revocation. This does not apply where the Secretary of State considers that doing so would be contrary to the interests of national security (subsection (2)).

232 Subsection (3) allows the Secretary of State to exclude from what is laid before Parliament anything that might prejudice to an unreasonable degree any person's commercial interests or be contrary to the interests of national security if published.

Section 18: Monitoring of designated vendor directions

233 This section gives the Secretary of State the power to issue a monitoring direction to Ofcom requiring Ofcom to obtain information relating to a provider's compliance with a designated vendor direction and to report this information to the Secretary of State. This section also makes provision for the Secretary of State to publish or disclose Ofcom's reports.

234 The section inserts new sections 105Z12 and 105Z13 into the 2003 Act.

Section 105Z12: Monitoring of designated vendor directions

235 Subsection (1) enables the Secretary of State to give Ofcom a monitoring direction requiring Ofcom to obtain information relating to a provider's compliance with a designated vendor direction (given under section 105Z1) and to provide information in a report to the Secretary of State. Ofcom will be engaged in information collection and provision only. The Secretary of State will be responsible for compliance decisions.

236 Subsection (2) sets out the nature of the information which Ofcom may be required to obtain under subsection (1).

237 Subsection (3) states that a monitoring direction may prescribe the form and content of the report to be provided by Ofcom under subsection (1). Ofcom may be required to set out their analysis in the report (subsection (4)) and may be required to provide the Secretary of State with separate reports on different matters, such as in relation to different direction requirements or in relation to plans (subsection (5)).

238 Subsection (6) states that Ofcom may be required to report to the Secretary of State at specified times and/or intervals.

239 Subsection (7) requires Ofcom to use their powers to obtain information in an appropriate manner when preparing a report under this section.

240 Subsection (8) allows the Secretary of State to give Ofcom more than one monitoring direction in relation to a designated vendor direction.

241 Subsection (9) allows the Secretary of State to vary or revoke a monitoring direction.

242 Subsection (10) states that the Secretary of State is required to consult with Ofcom before issuing or varying a monitoring direction.

Section 105Z13: Reports made under monitoring directions

243 Subsection (1) of section 105Z13 allows the Secretary of State to publish or disclose a report provided by Ofcom under section 105Z12.

244 Subsection (2) of section 105Z13 requires the Secretary of State to consider the need to keep certain matters confidential before publishing or disclosing a report. The definition of a confidential matter is set out in subsections (3) and (4).

Other provisions

245 Subsection (3) of section 18 amends section 135 of the 2003 Act so that Ofcom may require information from a person for the purpose of preparing a report required by a monitoring direction under section 105Z12.

246 Subsection (5) of section 18 amends section 393 so that nothing in that section prevents the publication or disclosure of a report under section 105Z13(1).

247 Subsection (6) of section 18 amends Schedule 8 so that decisions to require the provision of information for the purposes of preparing a monitoring report under section 105Z12 are not subject to appeal to the Competition Appeal Tribunal.

Section 19: Monitoring directions: inspection notices

248 This section gives Ofcom the power to give providers inspection notices for the purpose of obtaining information that would assist the Secretary of State in determining whether a provider has complied, or is complying with, requirements imposed by a designated vendor direction. It sets out how the power can be exercised and how compliance can be enforced.

249 The section inserts new sections 105Z14 to 105Z17 into the 2003 Act.

Section 105Z14: Power of Ofcom to give inspection notices

250 Subsection (2) allows Ofcom to give inspection notices to providers where the Secretary of State has given Ofcom a monitoring direction under section 105Z12. Ofcom may only exercise this power for the purpose of obtaining information which they are required to obtain by a monitoring direction under section 105Z12. Inspection notice powers can only be used to gather information from providers that directly relates to assisting the Secretary of State with determining whether a provider has complied, or is complying with requirements imposed by a designated vendor direction.

251 An inspection notice may impose a duty on the provider to take any number of actions set out in subsection (4), which include a duty to make persons available for interview and a duty to permit authorised persons (e.g. Ofcom employees) to enter specified premises (although not domestic premises) (subsection (5)).

252 Subsection (6) states that an inspection notice may not require the provider to take actions that would violate legal privilege or to disclose information or documents that are prohibited from being disclosed by or under an enactment mentioned in section 105A(4).

253 Subsection (7) states that an inspection notice must state the time in which each duty imposed by the notice must be complied with. An inspection notice cannot require a provider to do anything for a period of 28 days from the date the notice is given (subsection (8)).

Section 105Z15: Inspection notices: further provision

254 Subsection (1) states that an inspection notice must set out the consequences of failing to comply with a duty imposed by the notice.

255 Subsection (2) states that Ofcom may revoke an inspection notice or vary it to make it less onerous by notifying the provider.

256 Subsection (3) states that a provider may not act in a way which might defeat the purpose of an inspection notice once the notice is given, for example by destroying relevant documents.

257 Subsection (4) states that the reasonable costs incurred by Ofcom in connection with obtaining information under an inspection notice must be paid by the provider.

Section 105Z16: Inspection notices: information about entering premises

258 This section requires Ofcom to state in their annual report the number of occasions premises have been entered that year pursuant to a requirement under an inspection notice.

Section 105Z17: Inspection notices: enforcement of compliance

259 Subsection (1) states that sections 96A to 100, 102 and 103 of the 2003 Act, which apply to contraventions of conditions set under section 45, also apply in relation to a contravention of a duty imposed by an inspection notice (for an explanation of these sections, see the explanatory notes for section 105S above). Subsection (1) is subject to subsections (3) and (4), which provide for the maximum penalties that may be imposed in relation to a contravention of a duty imposed by an inspection notice, or a contravention of the duty not to act in a way that might defeat the purpose of an inspection notice.

260 Subsection (5) gives the Secretary of State a power to amend the amounts of maximum penalty set out in subsections (3) and (4). Regulations made using this power must be laid before Parliament in draft and approved by a resolution in each House (subsection (6)).

Other provisions

261 Subsection (5) of section 19 amends Schedule 8 of the 2003 Act so that a decision to impose a duty under an inspection notice (section 105Z14) is not subject to appeal to the Competition Appeal Tribunal.

Section 20: Power of Secretary of State to enforce compliance with designated vendor directions etc.

262 This section gives the Secretary of State the power to enforce compliance with designated vendor directions under section 105Z1. The section sets out the process to be followed where the Secretary of State considers that a provider is not complying with the requirements of a direction. It outlines the penalties that can be imposed for non-compliance and how they will be enforced.

263 The section inserts new sections 105Z18 to 105Z21 into the 2003 Act.

Section 105Z18: Notification of contravention

264 Subsection (1) allows the Secretary of State to issue a notification of contravention to a provider where there are reasonable grounds to suspect the provider has contravened a requirement imposed by a designated vendor direction under section 105Z1 or a requirement to provide a plan under section 105Z7.

265 Subsection (2) outlines what a notification of contravention should contain. This includes the Secretary of State's determination, the deadline for representations in response, the steps the Secretary of State considers the provider should take to comply with the requirement or remedy the contravention, and the proposed penalty.

266 Subsections (3) and (4) state that a notice of contravention can be given in respect of more than one contravention, and that where this is the case, a separate penalty may be specified for each contravention.

267 Subsections (5), (6) and (7) provide that, where a contravention is continuing, a notification may be given for any period during which the contravention occurred. Only one penalty may be specified in a notification for a continuing contravention in respect of the period of contravention specified in the notification, although a daily penalty may also be specified for each day the contravention continues after: a confirmation decision has been given under section 105Z20 which requires immediate action; or the expiry of any period specified in the confirmation decision for compliance.

268 Subsection (8) provides that the Secretary of State may give a further notification in respect of the same contravention in certain circumstances, such as if the earlier notification has been withdrawn without a penalty having been imposed in respect of the notified contravention.

Section 105Z19: Amount of penalty

269 Subsection (1) requires a penalty specified under section 105Z18 to be appropriate and proportionate. The maximum amount is 10 percent of the turnover of the person's relevant business for the relevant period (subsection (2)), or, in the case of a penalty for a continuing contravention imposed under section 105Z18(7), £100,000 per day (subsection (3)).

270 Subsection (4) states that where the provider has contravened a requirement to provide a plan under section 105Z7, the maximum penalty is £10 million or, in the case of a continuing contravention, £50,000 per day.

271 Subsections (5) and (6) state that the Secretary of State may by regulations amend the maximum fixed and daily penalty amounts set out in this section by laying a draft of the regulations before Parliament, which needs to be approved by each House.

272 Subsection (7) states that for the purpose of calculating penalty amounts, the turnover of a person's relevant business for a specific period and what is to be treated as the relevant business are to be determined in accordance with the rules set out by order of the Secretary of State under section 97(3)(a) of the 2003 Act. Section 97(3)(a) provides that the turnover of a person's business shall be calculated in accordance with such rules as may be set out by order made by the Secretary of State.

273 Subsection (8) provides definitions for 'relevant business' and 'relevant period'.

Section 105Z20 Enforcement of notification

274 Subsections (1) and (2) provide that, where a provider has been given a notification of contravention under section 105Z18 and the period for making representations has expired, the Secretary of State may give the provider a decision which confirms the requirements in the notification ("a confirmation decision") or inform the provider that no further action will be taken.

275 Subsection (3) provides that a confirmation decision may not be given unless the Secretary of State is satisfied that the provider has contravened a requirement imposed by a designated vendor direction under section 105Z18 or a requirement to provide a plan under section 105Z7.

276 Subsections (4) and (5) state that a confirmation decision must be given without delay and that it must include reasons for the decision.

277 Subsection (6) states that a confirmation decision may require the provider to immediately comply with the requirement being contravened and/ or remedy the consequences of the contravention, or specify a time period within which this must be done.

278 Subsection (7) states that the confirmation decision may require the provider, within a specified period of time, to pay the penalty specified in the notification, or a lesser penalty that the Secretary of State considers appropriate in light of any representations received or steps taken to comply with the requirement.

279 Subsection (8) requires the recipient of a confirmation decision to comply with it.

280 Subsection (9) states the Secretary of State may enforce a provider's duty in civil proceedings via an injunction, specific performance of a statutory duty or any other remedy or relief.

Section 105Z21: Enforcement of penalty

281 Subsections (2), (3) and (4) set out the approach to the enforcement of penalties imposed under section 105Z20 in different jurisdictions.

282 Subsection (5) provides further details on how a penalty imposed under section 105Z20 will be treated by the courts in England, Wales and Northern Ireland when recovery action is taken.

Section 21: Urgent enforcement directions

283 This section gives the Secretary of State the power to issue an urgent enforcement direction in serious cases. It sets out when and how this power may be used and enforced.

284 The section inserts new sections 105Z22 to 105Z24 into the 2003 Act.

Section 105Z22: Urgent enforcement direction

285 Subsection (1) sets out the circumstances in which the Secretary of State may give an urgent enforcement direction. These are that: (a) there are reasonable grounds to believe that a person has contravened a requirement imposed by a designated vendor direction under section 105Z1 or a requirement not to disclose under section 105Z25; (b) the case is urgent; and (c) urgent action is appropriate.

286 Subsection (2) states that an urgent case is one which creates an immediate risk of (a) a serious threat to national security or (b) significant harm to the security of a public electronic communications network, service, or associated facility.

287 Subsection (3) sets out what an urgent enforcement direction must contain. For example, it must require the recipient to take steps that the Secretary of State considers appropriate for complying with the requirement or remedying the consequences of the contravention (subsection (4)).

288 Subsection (5) states that the requirement to give reasons for giving an urgent enforcement direction does not apply where the Secretary of State considers that specifying reasons in the direction would be contrary to the interests of national security.

Section 105Z23: Urgent enforcement direction: confirmation

289 Subsection (1) states that after giving an urgent direction the Secretary of State must confirm or revoke it as soon as reasonably practicable. The Secretary of State may modify the direction when confirming it (subsection (2)).

290 Subsection (3) states the criteria that must be met before the Secretary of State may confirm an urgent direction. In particular, there must be a contravention of a relevant requirement, and that contravention must have resulted in, or create, an immediate risk of (a) a serious threat to national security or (b) significant harm to the security of a public electronic communications network, service or associated facility.

291 Subsection (4) states that before confirming an urgent enforcement direction, the Secretary of State must notify the recipient and give them the opportunity to make representations.

292 Subsection (5) states what the notice confirming an urgent enforcement direction under subsection (4) must contain. In the case of giving reasons, this is subject to subsection (6) which states that the requirement for the Secretary of State to give reasons for confirming a direction and any modifications does not apply where the Secretary of State considers that specifying reasons in such a notice would be contrary to the interests of national security.

293 Subsection (7) states that after the Secretary of State has decided whether to confirm a direction it must notify the recipient as soon as reasonably practicable.

Section 105Z24: Urgent enforcement direction: enforcement

294 Subsection (1) states that the recipient of an urgent enforcement direction must comply with it.

295 Subsection (2) states that the duty to comply is enforceable in civil proceedings by an injunction, specific performance measure or other appropriate remedy or relief.

Section 22: Requirement not to disclose

296 This section gives the Secretary of State a power to require the recipients of certain documents given under sections 15 to 21 not to disclose them if doing so would be contrary to the interests of national security. It also gives the Secretary of State the power to prevent disclosure of consultations. It makes provision for the enforcement of these powers by adopting and adapting the Secretary of State's powers to enforce compliance described at section 20.

297 The section inserts new sections 105Z25 and 105Z26 into the 2003 Act.

Section 105Z25: Requirement not to disclose

298 Subsections (1) and (2) give the Secretary of State the power to require the recipients of the following documents not to disclose their contents without the permission of the Secretary of State: designated vendor directions given under section 105Z1 and designation notices given under section 105Z8.

299 Subsections (3), (4), (5) and (6) give the Secretary of State the power to require the recipients of the following documents not to disclose their existence or contents without the permission of the Secretary of State: notifications of contravention under section 105Z18; confirmation decisions under section 105Z20; urgent enforcement directions under section 105Z22; or confirmation of urgent enforcement directions under section 105Z23.

300 Subsections (7) and (8) provide that the Secretary of State may only exercise the above power where the Secretary of State considers that it would be contrary to the interests of national security for the contents of (or, as the case may be, existence of) the document to be disclosed (except as permitted by the Secretary of State).

301 Subsection (9) gives the Secretary of State the power to require a person consulted about designated vendor directions or designation notices (or variations of the same) not to disclose anything about the consultation (or part of the consultation) without the permission of the Secretary of State. The Secretary of State may only exercise this power where the Secretary of State considers that it would be contrary to the interests of national security for these matters to be disclosed (subsection (10)).

302 Subsection (11) states that where a person is subject to a non-disclosure requirement, disclosure by an employee of that person or by a person engaged in the person's business will be regarded as a disclosure by the person, unless they can show that they took all reasonable steps to prevent disclosure.

Section 105Z26: Enforcement of requirement not to disclose

303 This section makes provision for the enforcement of the requirement not to disclose information which may be imposed under section 105Z25.

304 Subsection (1) provides that the Secretary of State's powers to enforce compliance with designated vendor directions described at section 20 also apply in relation to contraventions of a requirement not to disclose information imposed under section 105Z25.

305 Subsections (2) to (6) tailor the enforcement measures described at section 20 for the purposes of this section by making various substitutions and insertions. Most of the amendments are practical changes which are necessary to make the enforcement provisions workable in the context of the requirement not to disclose. Subsection (3) provides that, for the purposes of this section, the maximum penalty is £10 million or, in the case of a continuing contravention, £50,000 per day.

Section 23: Power of Secretary of State

306 This section gives the Secretary of State a power to require information from persons who are or have been providers, or any other person who appears to have information relevant to the exercise of the Secretary of State's functions under sections 105Z1 to 105Z26 of the Act. The section outlines the types of information that may be required, as well as the restrictions on this power and how it is to be enforced.

307 The section inserts new sections 105Z27 to 105Z29 into the 2003 Act.

Section 105Z27: Power of Secretary of State to require information etc

308 Subsection (1) gives the Secretary of State the power to require a person to provide such information as may be reasonably required for the purpose of exercising the Secretary of State's functions under sections 105Z1 to 105Z26.

309 Subsection (2) lists the persons who may be required to provide information, namely persons who are or have been providers or any other person who appears to have information relevant to the Secretary of State's functions under sections 105Z1 to 105Z26.

310 Subsection (3) describes what the Secretary of State may require a person falling under subsection (2) to do. This includes producing, generating, obtaining, collecting, retaining, processing, collating or analysing information.

311 Subsection (4) describes the type of information which the Secretary of State can require persons to provide. It can include, among other things, information about the use or proposed use of goods, services or facilities supplied by a particular person or information about goods, services or facilities proposed to be supplied by a particular person.

312 Subsection (6) allows the Secretary of State to specify how and when persons must comply with a requirement to provide information.

Section 105Z28: Restrictions on imposing information requirements

313 Subsection (2) states that the Secretary of State must request information under section 105Z27 by way of a notice which (a) describes the information required and (b) sets out the reasons for requiring it.

314 Subsection (3) states that the Secretary of State may only impose a requirement under section 105Z27(3) by way of a notice which sets out the requirement and the Secretary of State's reasons for imposing it.

315 Subsection (4) states that the Secretary of State does not need to set out the reasons for requiring the information specified in an information notice where doing so would be contrary to the interests of national security.

316 Subsection (5) states that the Secretary of State must only require information under section 105Z27 where the demand is proportionate.

317 Subsection (6) states that the Secretary of State is not to impose a requirement on a person under 105Z27(3) (i.e. a requirement to produce, generate, obtain, collect, retain, process, collate or analyse information), except where the imposition of the requirement is proportionate to the use to which the information is to be put in carrying out the Secretary of State's functions.

318 Subsection (7) states that the requirement to provide information under section 105Z27 does not require a person to disclose information that is legally privileged.

Section 105Z29: Enforcement of information requirements

319 Subsection (1) provides that the Secretary of State's powers to enforce compliance with designated vendor directions described at section 20 also apply in relation to the enforcement of information requirements under section 105Z27.

320 Subsection (2) provides that the maximum penalty for contraventions of an information request is £10 million or, in the case of a continuing contravention, £50,000 per day.

321 Subsection (3) gives the Secretary of State a power to change these amounts of maximum penalty by regulations. These regulations must be laid before Parliament that have to be approved by a resolution of each House.

Section 24: Further amendments concerning penalties

322 This section amends the 2003 Act in relation to the maximum amounts of penalties. It increases the maximum penalty which may be given for failing to provide information to Ofcom where Ofcom considers that the information is necessary for the purpose of carrying out their functions under sections 105L to 105Z, or preparing a report under section 105Z12.

323 The section inserts new section 139ZA into the 2003 Act.

Section 139ZA: Higher penalties for certain contraventions

324 Subsection (1) provides that where a person is given a notification of contravention under section 138 of the 2003 Act, there are two situations in which higher penalties apply:

- The first situation is where the proposed penalty is for a contravention of a requirement to provide information under section 135 and the information is necessary for Ofcom to carry out its functions under sections 105L to 105Z or to prepare a report under section 105Z12 (subsection (2)).

- The second situation is where the proposed penalty is for a contravention of a requirement imposed under subsection (3C) of section 135 (see section 12(3)(c) of the Act) (subsection (3)).

325 Subsection (4) sets out the higher penalty, namely a maximum penalty of £10 million or £50,000 per day for a continuing contravention.

326 Subsection (5) gives the Secretary of State a power to change these amounts of maximum penalty by regulations. These regulations must be laid before Parliament that have to be approved by a resolution of each House (subsection (6)).

Section 25: Further consequential amendments

327 This section makes minor amendments to the 2003 Act.

Section 26: Financial provisions

328 This section recognises that, as a matter of House of Commons procedure, a financial resolution needed to be agreed for the Bill from which the Act resulted.

Section 27: Extent

329 This section explains the territorial extent of the provisions in the Act. The Act will extend to England and Wales, Scotland and Northern Ireland.

Section 28: Commencement

330 This section explains when the provisions in the Act will come into effect.

331 Subsection (1) lists the provisions that will come into force on the day on which the Act is passed.

332 Subsection (2) lists the provisions that will come into force pursuant to separate commencement regulations, which may specify different dates for different purposes (subsection (3)).

Section 29: Short title

333 This section states that the Act may be cited as the Telecommunications (Security) Act 2021.

Commencement

334 Section 28 provides for the commencement of the provisions in this Act.

335 Subsection (1) provides that the following provisions of the Act will come into force on the day in which the Act is passed: sections 1 and 2 (so far as they confer power to make regulations); section 3 (so far as it confers power to issue a code of practice); sections 14 to 23; section 24 (so far as it relates to section 18); and sections 25(1) and (3), 26, 27, 28 and 29.

336 Subsection (2) provides that the following provisions of the Act will be brought into force by regulations made by the Secretary of State: sections 1 to 3 (so far as not already in force by virtue of subsection (1)), sections 4 to 13, section 24 (so far as not already in force by virtue of subsection (1)), and section 25(2).

337 Subsection (3) provides that different days may be appointed for different purposes.

338 Subsection (4) provides that the Secretary of State may by regulations made by statutory instrument make transitional, transitory or saving provision in connection with the coming into force of any provision of the Act.

Related documents

339 The following documents are relevant to the Act and can be read at the stated locations:

- UK Telecoms Supply Chain Review - https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/819469/CCS001_CCS0719559014-001_Telecoms_Security_and_Resilience_Accessible.pdf
- Future Telecoms Infrastructure Review - https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/732496/Future_Telecoms_Infrastructure_Review.pdf
- The Communications Act 2003 - https://www.legislation.gov.uk/ukpga/2003/21/contents
- Directive of the European Parliament establishing the European Electronic Communications Code - https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018L1972&from=EN
- NCSC advice on the use of equipment from High Risk Vendors in the UK's Telecoms Networks (Updated in July 2020) - https://www.ncsc.gov.uk/guidance/ncsc-advice-on-the-use-of-equipment-from-high-risk-vendors-in-uk-telecoms-networks
- Impact Assessment - The Telecommunications (Security) Act 2020: telecoms security requirements - https://publications.parliament.uk/pa/Acts/cAct/58-01/0216/IA%20Telecommunications_Security_Act_2020___The_Telecoms_Security_legislation.pdf
- Impact Assessment - The Telecommunications (Security) Act 2020: National Security powers in relation to high risk vendors - https://publications.parliament.uk/pa/Acts/cAct/58-01/0216/IA%20Telecommunications_Security_Act_2020___National_security_powers_in_relation_to_high_risk_vendors_.pdf
- House of Commons Defence Committee, "The Security of 5G", Second Report of Session 2019–21 HC 201 - https://committees.parliament.uk/publications/2877/documents/27899/default/

Annex A – Definitions

340 This Annex describes the scope of certain sections of the Act with reference to other sections of the 2003 Act.

341 Sections 1 to 14 concern 'providers of public electronic communications networks' and 'providers of public electronic communications services'. In these explanatory notes' description of those sections the term 'provider' has been used to describe both categories for ease of reference.

342 These terms are defined in the 2003 Act, in summary, as follows.

343 **Electronic communications network** is defined in section 32(1) of the 2003 Act as a transmission system for the conveyance, by the use of electrical, magnetic or electro-magnetic energy of signals of any description, and associated apparatus, software and stored data.

344 Examples of such networks include satellite networks, fixed networks (whether circuit- or packet-switched, and including the Internet) and mobile terrestrial networks and networks used for radio and television broadcasting, including cable TV networks.

345 **Electronic communications service** is defined (from 21 December 2020, when a new definition took effect following transposition of the European Electronic Communications Code) in section 32(2) of the 2003 Act as an internet access service, a number-based interpersonal communications service, or any other service consisting in, or having as its principal feature, the conveyance of signals, provided by means of an electronic communications network except in so far as it is a content service.

346 Examples of such services include telecommunications services and transmission services in networks used for broadcasting.

347 Section 151 of the 2003 Act defines a public **electronic communications network** as an electronic communications network provided wholly or mainly for the purpose of making electronic communications services available to the public.

348 This definition includes networks or services that serve business customers and those who serve individual customers. This definition does not include 'private networks' that provide internal communications within a network.

349 Section 15 provides that a 'designated vendor direction' may be given to a **public communications provider**. This term is defined in section 151 of the Communications Act 2003 as:

- a provider of a public electronic communications network;
- a provider of a public electronic communications service; or
- a person who makes available facilities that are associated facilities by reference to a public electronic communications network or a public electronic communications service.

350 In these explanatory notes, the term 'provider' has been used instead of public communications provider for ease of reference.

351 **Associated facility** is defined in section 32(3) of the 2003 Act as a facility, element or service which is available for use in association with an electronic communications network or service in order to make the provision of that network or service (or other services) possible, or to support the provision of other services.

352 Examples of such facilities include physical infrastructure of conditional access systems and electronic programme guides.

Annex B – Hansard references

353 The following table sets out the dates and Hansard references for each stage of the Act's passage through Parliament.

Stage	Date	Hansard Reference
House of Commons		
Introduction	24 November 2020	Vol. 684 Col. 715
Second Reading	30 November 2020	Vol. 685 Col. 70
Public Bill Committee	14 January 2021	1st sitting
		2nd sitting
	19 January 2021	3rd sitting
		4th sitting
	21 January 2021	5th sitting
		6th sitting
	26 January 2021	7th sitting
		8th sitting
Report and Third Reading	25 May 2021	Vol. 696 Col. 278
House of Lords		
Introduction	26 May 2021	Vol. 812 Col. 1087
Second Reading	29 June 2021	Vol. 813 Col. 707
Grand Committee	13 July 2021	Vol. 813 Col. 460GC
	15 July 2021	Vol. 813 Col. 520GC
Report	19 October 2021	Vol. 815 Col. 72
Third Reading	26 October 2021	Vol. 815 Col. 647
Commons Consideration of Lords Amendments	8 November 2021	Vol. 703 Col. 109
Lords Consideration of Commons Reasons	15 November 2021	Vol. 816 Col. 22
Royal Assent	17 November 2021	House of Commons Vol.703 Col. 623
	17 November 2021	House of Lords Vol. 816 Col. 278

Printed and published in the UK by The Stationery Office Limited under the authority and superintendence of Jeff James, Controller of Her Majesty's Stationery Office and Queen's Printer of Acts of Parliament.

tso
a Williams Lea company

Published by TSO (The Stationery Office), a Williams Lea company, and available from:

Online
www.tsoshop.co.uk

Mail, Telephone, Fax & E-mail
TSO
PO Box 29, Norwich, NR3 1GN
Telephone orders/General enquiries: 0333 202 5070
Fax orders: 0333 202 5080
E-mail: customer.services@tso.co.uk
Textphone: 0333 202 5077

TSO@Blackwell and other Accredited Agents

ISBN 978-0-10-560260-6

9 780105 602606