PRODUCT SECURITY AND TELECOMMUNICATIONS INFRASTRUCTURE BILL

EXPLANATORY NOTES

What these notes do

These Explanatory Notes relate to the Product Security and Telecommunications Infrastructure Bill as introduced in the House of Commons on 24 November 2021 [Bill 199].

- These Explanatory Notes have been prepared by the Department for Digital, Culture, Media and Sport in order to assist the reader of the Bill and to help inform debate on it. They do not form part of the Bill and have not been endorsed by Parliament.
- These Explanatory Notes explain what each part of the Bill will mean in practice; provide background information on the development of policy; and provide additional information on how the Bill will affect existing legislation in this

area.

- These Explanatory Notes might best be read alongside the Bill. They are not, and are not intended to be, a comprehensive description of the Bill.

Table of Contents

Subject	Page of these Notes
Overview of the Bill	9
Policy background	9
Legal background	23
Part 1: Product Security	23
Part 2: Telecommunications Infrastructure	23
Territorial extent and application	25
Commentary on provisions of Bill	27
Part 1: Product Security	27
Chapter 1: Security requirements	27
Clause 1: Power to specify security requirements	27
Clause 2: Further provision about regulations under section 1	28
Clause 3: Power to deem compliance with security requirements	30
Clause 4: Relevant connectable products	30
Clause 5: Types of product that may be relevant connectable products	31
Clause 6: Excepted products	34
Clause 7: Relevant persons	37

Chapter 2: Duties of relevant persons 41
Clause 8: Duty to comply with security requirements 41
Clause 9: Statements of compliance 42
Clause 10: Duty to investigate potential compliance failures 46
Clause 11: Duties to take action in relation to compliance failure 47
Clause 12: Duty to maintain records 49
Clause 13: Duties to take action in relation to manufacturer's compliance failure 50
Clause 14: Duty to comply with security requirements 51
Clause 15: Statements of compliance 52
Clause 16: Duty not to supply products where compliance failure by manufacturer 53
Clause 17: Duty to investigate potential compliance failures of importer or manufacturer 54
Clause 18: Duties to take action in relation to importer's compliance failure 55
Clause 19: Duties to take action in relation to manufacturer's compliance failure 56
Clause 20: Duty to maintain records of investigations 58
Clause 21: Duty to comply with security requirements 60

Clause 22: Statements of compliance 60
Clause 23: Duty not to supply products where compliance failure by manufacturer 61
Clause 24: Duties to take action in relation to distributor's compliance failure 62
Clause 25: Duties to take action in relation to manufacturer's compliance failure 63
Chapter 3: Enforcement 67
Clause 26: Enforcement of Part 1 67
Clause 27: Delegation of enforcement functions 69
Clause 28: Compliance notices 70
Clause 29: Stop notices 72
Clause 30: Recall notices 73
Clause 31: Power to vary or revoke enforcement notices 77
Clause 32: Failure to comply with enforcement notice 79
Clause 33: Appeals against enforcement notices 81
Clause 34: Compensation for notices wrongly given 83
Clause 35: Appeals against decisions under section 34 85
Clause 36: Monetary Penalties 87
Clause 37: Determining the amount of a penalty 88
Clause 38: The relevant maximum 88

Clause 39: Penalty notices: further provision 89
Clause 40: Enforcement of penalty notices 91
Clause 41: Appeals against penalty notices 91
Clause 42: Forfeiture 93
Clause 43: Further provision about forfeiture 95
Clause 44: Appeal against decision under section 42 96
Clause 45: Power to inform public about compliance failures 97
Clause 46: Power to publish details of enforcement action taken against relevant persons 97
Clause 47: Power to recall products 98
Clause 48: Disclosure of information 99
Clause 49: Offence of purporting to act as authorised to exercise enforcement function 101
Clause 50: Means of giving notices 101
Clause 51: Liability of authorised representatives 102
Clause 52: Offences by directors, partners etc 102
Chapter 4: Supplementary provision 103
Clause 53: Guidance 103
Clause 54: Meaning of “UK consumer connectable product” 104
Clause 55: Meaning of “supply” 108

Clause 56: Meaning of other expressions used in Part 1 117
Part 2: Telecommunications Infrastructure 118
Clause 57 : Meaning of “occupier” in relation to land occupied by an operator [J500a] 118
Clause 58: Rights under the electronic communications code to share apparatus 119
Clause 59: Upgrading and sharing of apparatus: subsisting agreements 122
Clause 60: Upgrading and sharing of apparatus installed before December 2003 126
Clause 61: Rent under tenancies conferring code rights: England and Wales 127
Clause 62: Rent under tenancies conferring code rights: Northern Ireland 129
Clause 63: Compensation relating to code rights: England and Wales 131
Clause 64: Compensation relating to code rights: Northern Ireland 132
Clause 65: Jurisdiction of court in relation to tenancies in England and Wales 133
Clause 66: Unresponsive Occupiers 133

Clause 67: Arrangements pending determination of certain applications under code 148
Clause 68: Use of alternative dispute resolution 149
Clause 69: Complaints relating to the conduct of operators 152
Clause 70: Power to impose time limits on the determination of code proceedings 152
Clause 71: Rights of network providers in relation to infrastructure 153
Clause 72: Power to make consequential amendments 156
Clause 73: Meaning of "electronic communications code" 157
Part 3: Final Provisions 157
Clause 74: Power to make transitional or saving provision 157
Clause 75: Regulations 157
Clause 76: Extent 158
Clause 77: Commencement 158
Clause 78: Short title 159
Schedule: Unresponsive occupiers: consequential amendments 159
Commencement 160

Financial implications of the Bill 160

Parliamentary approval for financial costs or for charges imposed 161

Compatibility with the European Convention on Human Rights 162

Related documents 163

Annex- Territorial extent and application in the United Kingdom 164

Overview of the Bill

1 The Bill creates a new regulatory scheme to make consumer connectable products ("smart" products) more secure against cyber attacks. It also contains provisions intended to accelerate the deployment and expansion of mobile, full fibre and gigabit capable networks across the UK through changes to legislation (including changes to the Electronic Communications Code) that deal with the rights of Code operators to install, maintain and use electronic communications apparatus.

Policy background

2 The government is committed to improving connectivity and ensuring all premises can achieve a good broadband speed. Gigabit-capable broadband is enabling infrastructure which will drive UK economic growth. It is the backbone of 5G mobile connectivity, which allows quick digital transactions and services which, in turn, will encourage innovation and enable personalised, efficient delivery of public services. The Covid pandemic showed that

being connected helped businesses to run, families stay in touch, allowed children to keep up with their education and supported society to function at a time of crisis.

3 Greater connectivity will increase the demand for consumer connectable products such as smart speakers, smart TVs and wearable technology and the digital services they enable. Currently, the average UK household already has nine consumer connectable products in their home, with many lacking basic cyber security protections. Poorly secured consumer connectable products threaten individuals' online security, and subsequently, their privacy and safety.

4 When security flaws of products in the home are exploited, significant problems can ensue. Devices with weak security can be compromised, and be used in large-scale cyber attacks, such as Distributed Denial of Service ("DDoS") attacks. The impact of such attacks can reverberate across the wider UK, and global, economy.

5 The government is committed to protecting UK consumers from cyber threats and preventing the economic loss that results from attacks of this kind (estimated at over £1 billion per annum). To protect consumers, legislation to improve connectivity is paired with legislation to improve consumer-facing cyber security. The Product Security and Telecommunications Infrastructure Bill has been designed to improve the UK's resilience to cyber attacks, and improve connectivity for individuals and businesses across the UK.

Product Security

6 Consumer connectable products are consumer products which can connect to the internet or other networks, and can transmit and receive digital data. Examples of these products include smartphones, smart TVs, smart speakers, connected baby monitors and connected alarm systems. They are also known as consumer "Internet of Things devices" ("consumer IoT") or consumer "smart" devices. In 2020, there were an estimated 12.9

billion consumer connectable products worldwide.[1]

7 As electrical products they are subject to product safety regulation including the Consumer Protection Act 1987 and the General Product Safety Regulations 2005 [SI 2005/1803]. To ensure these products do not create radio interference, many of them are also subject to the Radio Equipment Regulations 2017 [SI 2017/1206]. The existing regimes, however, do not create any provision that minimum security requirements relating to products must be met.

8 Insecure products can be used in ways not intended by the consumer, such as the case of security cameras being compromised in Singapore.[2] In addition, insecure products can act as the 'point of entry' across a network, enabling attackers to access valuable information, such as the attackers who were able to access a US casino's customers'

[1] Gartner, 2017, https://www.gartner.com/newsroom/id/3598917

[2] The Straits Times. 2020. https://www.straitstimes.com/singapore/singapore-home-cams-hacked-and-stolen-footage-sold-on-pornographic-sites

details via a connected thermometer in a fishtank.[3]

9 Devices can be compromised at scale as part of Distributed Denial of Service (DDOS) or 'botnet' attacks. For example, in 2016 cyber criminals compromised 300,000 products with the Mirai malware. The attackers utilised the collective computing power to successfully disrupt the service of many news and media websites including the BBC and Netflix. The Mirai malware was able to penetrate so many devices due to widespread weak security features (such as default passwords).

10 In 2017 and 2018, a range of vulnerabilities were identified in the web service that connected to a smart watch brand that is marketed at children.[4] The vulnerabilities allowed an attacker to access personally identifiable information including the linked mobile phone number and GPS coordinates

[3] The Washington Post. 2017. https://www.washingtonpost.com/news/innovations/wp/2017/07/21/how-a-fish-tank-helped-hack-a-casino/

[4] Norwegian Consumer Council, press release, 2017 https://www.forbrukerradet.no/side/significant-security-flaws-in-smartwatches-for-children/

for each watch. The penetration testers who had found the vulnerability were unable to contact the manufacturer to report their concerns meaning watch users - including children - continued to be exposed to harm. The total number of users of these smart watches was determined to be around 1 million globally.

11 UK consumers are rarely able to make security conscious choices at the point of purchase due to a lack of information and so cannot easily protect themselves from cyber threats. A 2020 UCL study surveyed 270 common consumer connectable products and found that consumers were not given clear information outlining how long their connectable product would be supported with security software updates for. Without clear information, consumers' overwhelmingly assume that a product is secure because it is for sale, so vulnerable devices see continued use[5] in homes where the consumer has no

[5] The cheap security cameras inviting hackers into your home, Which, 2019

idea that the product represents a risk.

12 In response to growing concerns about the vulnerability of baby monitors and domestic CCTV cameras to hacking, the National Cyber security Centre ("NCSC") issued a warning and guidance for consumers to adjust the security settings of products they purchase.[6]

13 Going further, the government committed to ensuring "the majority of online products and services coming into use become 'secure by default' by 2021" in its 2016 National Cyber Security Strategy.[7] In March 2018 the government consulted on its Secure by Design Report[8] and this was followed with the publication of the voluntary Code of Practice for Consumer IoT Security[9] in October 2018 which recognised the ever growing number and types of consumer connectable products.

https://www.which.co.uk/news/2019/10/the-cheap-security-cameras-inviting-hackers-into-your-home/

[6] Smart camera and baby monitor warning given by UK's cyber-defender, BBC, 2020 https://www.bbc.co.uk/news/technology-51706631

[7] National Cyber Security Strategy, November 2016 https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021

[8] Secure by Design report, March 2018 https://www.gov.uk/government/publications/secure-by-design-report

[9] Code of Practice for Consumer IoT Security, October 2018 https://www.gov.uk/government/publications/code-of-practice-for-consumer-iot-security

The code shifted the approach to securing devices by moving the burden away from consumers and instead used policy to encourage security features to be built into products at the design stage.

14 Building on its domestic work the government sought to find an international consensus on how to better secure consumer connectable products. Following a partnership with both countries, Australia's Department of Home Affairs (2020)[10] and India's Department for Telecommunications (2021)[11] have both published Codes of Practice that are consistent with the thirteen principles that the UK first published in 2018.

15 The government has also worked with the European Telecommunications Standards Institute ("ETSI") to create a new globally applicable standard EN 303 645: Cyber Security for Consumer Internet of Things:

[10] Code of Practice: Securing the Internet of Things for Consumers; Australian Government (2020) https://www.homeaffairs.gov.au/reports-and-pubs/files/code-of-practice.pdf

[11] Code of Practice for Securing Consumer Internet of Things TEC 31318, Government of India (2021) https://tec.gov.in/pdf/M2M/Securing%20Consumer%20IoT%20_Code%20of%20pratice.pdf

Baseline Requirements which is consistent with the 13 principles of the UK's Code of Practice. ETSI has over nine hundred members from 65 countries. Adopted in June 2020, EN 303 645 is the first globally-applicable technical standard for the cyber security of consumer connectable products.

16 While the government encouraged industry to adopt the guidelines in the UK's Code of Practice for Consumer IoT Security, voluntary compliance was slow, and poor security practices remain commonplace. At the time of its publication in 2018, the Internet of Things Security Foundation estimated that 9 per cent of manufacturers maintained an adequate vulnerability disclosure programme. By 2019, the figure was still only 13 per cent.[12]

17 In May 2019, the government launched a consultation on legislative proposals for the cyber security of consumer connectable products. Responses to the consultation

[12] Understanding the Contemporary Use of Vulnerability Disclosure - 2020 Progress Report, IoT Security Foundation, 2020 https://www.iotsecurityfoundation.org/just-13-percent-of-consumer-iot-firms-allow-vulnerability-reporting-despite-incoming-laws-and-international-standards/

demonstrated widespread support for the introduction of a mandatory cyber security baseline aligned with priority security requirements as outlined in the Code of Practice.

18 The government published detailed proposals for regulating the cyber security of consumer connectable products as part of a Call for Views in July 2020. Responses to this Call for Views further supported the government's position, that widespread compliance to priority security requirements from EN 303 645 will have the greatest impact protecting UK consumers purchasing connectable products.[13]

19 The Bill creates powers for ministers to specify security requirements relating to consumer connectable products. Businesses involved in making these products available in the United Kingdom will need to comply with these requirements. The government intends

[13] Government response to the call for views on consumer connected product cyber security legislation, April 2021 https://www.gov.uk/government/publications/regulating-consumer-smart-product-cyber-security-government-response

to use these powers to place three of the original security requirements in the 2018 Code of Practice, and EN 303 645, on a statutory footing. These new statutory security obligations will include a ban on the use of default passwords, a requirement for manufacturers to manage the reporting of security vulnerabilities and a requirement for consumers to be told at the point of sale the minimum period of time that the product will receive security updates.

Telecommunications Infrastructure

20 The Future Telecommunications Infrastructure Review in 2018 established the importance of the UK telecommunications market to future economic growth. The review concluded that while the UK is a world leader in ‘superfast’ connectivity there were several barriers to deployment that inhibit widespread access to the next generation of gigabit-capable broadband. Gigabit broadband coverage is currently at 58% with coverage expected to rise to 60% by the end of 2021

preventing the UK from realising the full range of benefits digital connectivity creates. The government pledged to review the relevant policy and legal framework to identify ways to overcome any administrative and legal obstacles delaying broadband deployment.

21 The 2019 Conservative Party Manifesto pledged to ensure that everyone across the UK gets to enjoy the benefits of greater connectivity and promised to legislate to speed up UK digital connectivity. In November 2020 the government committed to deliver gigabit-capable broadband to 85 per cent of UK premises by 2025 to support digital growth and innovation.[14]

22 The government is working with industry to target a minimum of 85 per cent gigabit-capable UK coverage by 2025 and to get as close to 100 per cent as possible. The government is also aiming to ensure that 95 per cent of the UK's geographic landmass has 4G coverage from at least one mobile network operator by 2025 and that the majority of

[14] https://www.gov.uk/government/publications/national-infrastructure-strategy

the UK population has 5G coverage by 2027.

23 Rights to install, maintain, upgrade and share telecommunications apparatus are regulated by the Code. The Code was substantially reformed in 2017, with changes intended to make it cheaper and easier for operators to deploy, upgrade and share their apparatus. While improving the situation in some parts of the industry, subsequent government engagement highlighted that the 2017 reforms have not been working as intended in a number of key areas.

24 In January 2021, the government therefore ran a consultation on further reform of the Code. From this process the government identified that a number of reforms to the Code were needed to support delivery of the digital communications services that UK consumers and businesses need. These include:

- amendments to operator rights to upgrade and share their apparatus, to optimise the use of existing networks and reduce the need for additional installations;

- changes to support the renewal of expired Code agreements, to bring the process and renewal terms closer to those for new Code agreements;
- promotion of faster and more efficient negotiations by measures promoting the use of Alternative Dispute Resolution ("ADR"), to encourage collaboration and remove any incentive to delay the completion of Code agreements; and
- introduction of a streamlined process for cases where a landowner or occupier fails to respond to operator requests for Code rights.

25 In June 2020, DCMS ran a call for evidence on possible reforms to The Communications (Access to Infrastructure) Regulations 2016. Having a power to amend the Regulations will make them more useful for the digital infrastructure sector so that the impact achieved by the 2016 legislation keeps pace with innovation in the sector and the

original policy intent. Any changes will be made via the affirmative resolution procedure.

Legal background

Part 1: Product Security

26 This Bill includes a power to specify security requirements relating to relevant connectable products and creates obligations on economic actors such as manufacturers, importers and distributors in respect of compliance with those security requirements. The enforcement of these obligations will use powers provided for in Chapter 3, as well as existing powers in the Consumer Rights Act 2015 ("the 2015 Act"). The 2015 Act consolidates enforcers' powers as listed in Schedule 5 to investigate potential breaches of consumer law.

Part 2: Telecommunications Infrastructure

27 The Code is contained in Schedule 3A to the Communications Act 2003 ("the 2003 Act"), as inserted by the Digital Economy Act 2017 ("the 2017 Act"). The Code was previously

found in the Telecommunications Act 1984 (see Schedule 2 to that Act). The 2017 Act replaces that iteration with a new version of the Code (see Schedule 1 to the 2017 Act), which was inserted into the 2003 Act (as Schedule 3A to that Act).

28 The Electronic Communications Code (Jurisdiction) Regulations 2017 ("the 2017 Regulations") confer jurisdiction on the Upper Tribunal and First-tier Tribunal in respect of England and Wales, and on the Lands Tribunal for Scotland in respect of Scotland. References to "the court" or "a court" in these Notes are to be taken to refer to those tribunals and courts unless specified otherwise. The 2017 Regulations do not extend to Northern Ireland. Accordingly, all functions conferred by the Code on a court in Northern Ireland remain exercisable in Northern Ireland only by a county court. References to "the court" or "a court" in these Notes are therefore to be construed accordingly as regards Northern Ireland,

unless otherwise specified.

Territorial extent and application

29 Save as set out below, the Bill extends and applies to England and Wales, Scotland and Northern Ireland. In respect of Northern Ireland, the Bill is compatible with the Protocol on Ireland/Northern Ireland to the Agreement on the Withdrawal of the United Kingdom of Great Britain and Northern Ireland from the European Union and the European Atomic Energy Community.

30 In Part 2, clauses 61, 63 and 65 extend and apply to England and Wales only, as these clauses make amendments to the Landlord and Tenant Act 1954 which extends and applies only to England and Wales. Similarly, clauses 62 and 64 extend and apply to Northern Ireland, as they amend the Business Tenancies (Northern Ireland) Order 1996 which extends and applies only to Northern Ireland.

31 Section C10 of Schedule 5 to the Scotland

Act 1998, section C9 of Schedule 7A to the Government of Wales Act 2006 and paragraph 29 of Schedule 3 to the Northern Ireland Act 1998 provide for telecommunications and wireless telegraphy to be reserved matters. Section C7 of Schedule 5 to the Scotland Act 1998 and section C6 of Schedule 7A to the Government of Wales Act 2006 provide for consumer protection to be a reserved subject matter, whilst paragraph 37 of Schedule 3 to the Northern Ireland Act 1998 provides for consumer safety in relation to goods to be a reserved subject matter. In the view of the UK Government, the subject matters of the provisions in the Bill are reserved subject matters in Scotland, Wales and Northern Ireland.

32 See the table in Annex A for a summary of the position regarding territorial extent and application in the United Kingdom.

Commentary on provisions of Bill

Part 1: Product Security

Chapter 1: Security requirements

Clause 1: Power to specify security requirements

33 Clause 1 provides the Secretary of State with the power to specify by regulations security requirements relating to connectable products, described in the Bill as relevant connectable products, or to connectable products of a specified description. These will apply to relevant persons or relevant persons of a specified description, for example, persons defined as a “manufacturer” in respect to a product.

34 Subsection (1) sets out limitations on using the power. The power must be used to protect or enhance the security of relevant connectable products made available to consumers in the United Kingdom or of the users of those products.

35 Subsection (4) points to provisions in other clauses (8, 14, and 21) that impose duties on

relevant persons in relation to connectable products to comply with security requirements.

Clause 2: Further provision about regulations under section 1

36 This clause makes further provision about how the Secretary of State may exercise the power under clause 1 of the Bill. Subsection (1) sets out that a security requirement may relate to all the products of a relevant person or a relevant person of a particular description.

37 Subsection (3) sets out a non-exhaustive list of what, in addition to a physical device, a security requirement may apply to. This list includes software related to a product which may or may not be installed on the product. The software may or may not be provided by the manufacturer of the product.

38 Subsection (4) establishes that the requirements may be ongoing, requiring a relevant person to act in relation to a connectable product after it has been made available in the United Kingdom.

39 Subsection (6) sets out that regulations under clause 1 are subject to the affirmative resolution procedure, unless they only make limited variations as specified in subsection (5), in which case the negative resolution procedure applies.

Example exercise of power: future security requirements

Security requirements will be technical in nature. They will set out details such as the products and software relevant to (and excluded from) each individual security requirement, technical detail and language describing what is required by each security requirement, and may mandate specific conformity assessment procedures in respect of certain products.

The initial security requirements are intended to align with the following intent:

Security Requirement 1 Ban universal default passwords

Security Requirement 2 Implement a means to manage reports of

vulnerabilities

Security Requirement 3 Provide transparency on for how long, at a minimum, the product will receive security updates

Clause 3: Power to deem compliance with security requirements

40 The security requirements set by the Secretary of State in regulations represent the minimum security requirements which must be complied with in relation to a product.Some persons may exceed these requirements, for example by wholly satisfying an international standard such as EN 303 645. This clause allows the Secretary of State to specify standards which, when complied with, will constitute deemed compliance with a security requirement by the relevant person. Subsection (3) sets out that this power will be subject to the negative resolution procedure.

Clause 4: Relevant connectable products

41 This clause defines “relevant connectable product” as a product that is an internet-connectable product or a network-connectable product as defined in clause 5, and which is not an “excepted product” specified in regulations made pursuant to clause 6, which empowers the Secretary of State to specify products that are not within the regulatory scope of this legislation.

Clause 5: Types of product that may be relevant connectable products

42 This clause defines the types of products that are relevant connectable products for the purposes of this legislation.

43 Subsections (1) and (2) define “internet-connectable products” as being capable of connecting to the internet using a communication protocol that forms part of the Internet Protocol suite to send or receive data over the internet.

44 Subsection (3) defines a “network-connectable product” as a product that is

capable of sending and receiving data transmitted using electronic or electromagnetic energy; is not an internet connectable product; and meets the connectability conditions set out in subsections (4) or (5).

45 Subsection (4) establishes the first connectability condition where a product is capable of connecting directly to an internet-connectable product by means of a communication protocol that forms part of the Internet Protocol suite. To meet this condition, these products must be capable of using a communication protocol that forms part of the Internet Protocol suite, but itself unable to connect directly to the internet.

46 Subsection (5) establishes the second connectability condition which covers the capability of a product connecting directly to two or more products at the same time by a communication protocol that does not form part of the Internet Protocol suite; and it being capable of connecting directly to an internet-connectable product by means of a

communication protocol which does not form part of the Internet Protocol suite, whether or not at the same time as it connects to any other product.

47 Subsection (6) establishes that a product which consists of wires and cables used merely to connect the relevant product to another product is not to be considered as a product for the purposes of the test established in subsection (5)(a). Subsection (8) confirms the involvement of a wire or cable does not stop a connection from occurring “directly” for the purposes of subsections (4) to (7).

48 Subsection (7) establishes that where two or more products are designed to be used together for the purposes of facilitating the use of a computer, at least one of the products (the “linking product”) can connect directly to an internet-connectable-product (the computer or some other product)) by means of a communication protocol that does not form part of the Internet protocol suite and each of the other products (the “input products”) are

capable of connecting to a “linking product” directly and wirelessly by a non-Internet Protocol suite communication protocol, then they are to be seen to meet the second connectability condition subsection (3).

Clause 6: Excepted products

49 This clause provides a power for the Secretary of State to specify in regulations connectable products to which Part 1 will not apply, but would otherwise be within the regulatory scope of this legislation. The government intends to except products from the regulatory scope of this legislation where it would not be appropriate for them to be included, for instance, where inclusion would subject them to double regulation.

50 Subsection (2) establishes that regulations may be made to specify rules for the excepted status of a “primary product” and a “secondary product” when they are incorporated into or attached to, or otherwise form part of, each other.

51 Regulations made by the power in this clause are subject to the negative resolution procedure when varying a description of a product, or, specifying any description of a product which is covered by equivalent requirements relating to security. All other regulations made under the Clause are subject to affirmative resolution procedure.

Example exercise of power: Future exceptions for the purposes of avoiding dual regulation

Smart metering devices. The government is not intending to except all smart metering products, but only those that are already subject to security requirements through Relevant Technical Specifications which must be met when subject to a Relevant Energy License Conditions as set out in The Gas Act 1986 (as amended) and The Electricity Act 1989 (as amended). The smart metering products the government intends to except are also covered by Commercial Product Assurance (CPA).

Smart chargepoints. The

government has stated that these will be subject to minimum security requirements using powers provided by the Automated and Electric Vehicles Act 2018.

Medical devices. The government regulates these through the Medical Devices Regulations 2002. As of September 2021, a consultation is underway on the future regulations of medical devices in the UK, including proposals to regulate certain software as medical devices.

Vehicles. Road vehicles are covered by the Road Traffic Act 1988. In September 2021, the government announced its intention to develop a national framework to modernise vehicle standards, including proposals for cyber security requirements, in the future of transport regulatory review.

Aviation is covered by a number of existing regulations and the government uses CAP1753 to achieve compliance with the various cyber security requirements. The Single Consolidated Direction 1/2021 is due to come into effect on 31

December 2021 and covers airports and carriers that fall within the National Aviation Security Programme. Unmanned Aircraft Systems are covered by CAP1789A: UAS Implementing Regulation.

Maritime is covered by a number of existing Maritime Security Regulations and the government kept the ISPS (International Ship and Port Facility) Code in force since EU Exit through the The Ship and Port Security (Amendment etc.) (EU Exit) Regulations 2019. At this time, SI 2019 No. 0308 amends 2004/0725 (Regulation), SI 2004 No. 1495, SI 2009 No. 2048 and revokes 2008/0324 (Regulation).

Clause 7: Relevant persons

52 This clause defines the economic actors to which the duties set out in Part 1 will apply. "Relevant persons" are defined as manufacturers, importers and distributors of relevant connectable products.

53 Subsection (3) defines “manufacturer” as a person who (i) manufactures a product, or has a product designed or manufactured, and (ii) markets that product under their own name or trade mark. A person who markets under their own name or trademark a product manufactured by another person is also a manufacturer.

54 Subsection (4) defines “importer” as a person who (a) imports the product into the United Kingdom from another country, and (b) is not a manufacturer of the product.

55 Subsection (5) defines “distributor” as any person who (a) makes the product available in the United Kingdom, and (b) is not a manufacturer or an importer of the product.

56 Subsection (6) provides that a person will not be considered a distributor if they make the product available by performing a contract for or including the installation of the product in a building or structure. This will only apply if products identical to the installed product are

or have been made available to consumers outside of such a contract for their installation.

Examples of when smart products are integrated into the performance of a contract

Scenario 1: An electrician is hired by a family to install a ‘smart’ sound control system in their home. The family purchased the product at a local electronics store and the electrician is only hired to install the products that form the smart sound system. The electrician is not considered to be a distributor because they had no part in the supply of the product (the electrician never owned the product so they did not ‘’make it available’’ to the family.

Scenario 2: An electrician is hired by a family to install a ‘smart’ sound system in their home. The family enters into a contract for the installation of the smart sound system and pays an agreed amount for the project. The electrician decides what specific products and components will be purchased and installed to meet the contract. The electrician buys and installs products that are normally sold

to consumers via an online consumer retail website. While the electrician owned the product and made it available to the family, the electrician will not be considered a distributor because products identical to the installed products have been made available to consumers via an online consumer retail website.

Scenario 3: A family hires a company ‘’A’’ to install a bespoke smart sound system in their home. The family pays for the entire project (including design, production, installation and the products). The products that form the smart sound system can only be purchased from company A as part of a contract that involves their installation. The products are unique and are not made available to consumers in any other way (e.g. they cannot be purchased from a shop without entering into a contract for their installation). Company A is a distributor of the products.

Intention for subsection (6)

This provision is intended to absolve small businesses whose ordinary

business is not the sale of products such as electricians, etc. from the potentially burdensome duties of distributors. At the same time, the provision ensures that products such as smart home control systems (which are in most cases only made available through a contract for their installation) are in scope and their users will be protected.

Chapter 2: Duties of relevant persons

Clause 8: Duty to comply with security requirements

57 This clause places an obligation on a manufacturer of a product to comply with any relevant security requirements relating to that product where one of two conditions is met. Subsection (2) sets out the first condition and establishes that the duty applies where the manufacturer intends for, is aware that, or ought to be aware that, the product will be a "UK consumer connectable product", which is defined in clause 54.

58 Subsection (3) sets out the second condition and ensures that this duty continues to apply when a product is in use by a customer (as it has become a “UK consumer connectable product”). The manufacturer has a duty to comply where the manufacturer intended, was aware, or ought to have been aware that the product would become a “UK consumer connectable product” at the point where the manufacturer made the product available.

Clause 9: Statements of compliance

59 This sets out that a manufacturer may not make a consumer connectable product available in the United Kingdom unless it is accompanied by (a) a statement of compliance or (b) a summary of the statement of compliance in which the manufacturer states that in its opinion it has complied with the applicable security requirements.

60 Subsection (4) defines “applicable security requirements" as any relevant security requirements relating to a product to which the

manufacturer is subject. In this clause ‘’applicable security requirements’’ are likely to be any security requirement that apply to the manufacturer before a product is made available to the market. Some security requirements will only apply after a product is made available in the United Kingdom and may not be applicable security requirements for the purpose of the statement of compliance. It is a breach of this duty to make a product available in the United Kingdom if the product is not accompanied by a statement of compliance or a summary statement of compliance and should have been, even if the manufacturer has technically complied with applicable security requirements relating to that product.

61 Subsection (2)(b) defines a “summary statement of compliance” as a summary of the statement of compliance that is in such a form, and contains such information, as specified in regulations made by the Secretary of State.

62 Subsection (3) defines a statement of

compliance, in relation to a product, as a document that meets the following conditions. A statement of compliance must state that, in the opinion of the manufacturer, any applicable security requirements have been complied with. The statement must be prepared by or on behalf of the manufacturer, and be in a form, or contain any information, specified in regulations made by the Secretary of State under subsection (6).

63 Subsection (5) covers cases where a product has more than one manufacturer. In such cases, all manufacturers may jointly prepare a statement of compliance but it is also possible for a single manufacturer to prepare a statement of compliance. The statement of compliance must contain all necessary information for the duty to be discharged.

64 Subsection (6) provides a power for the Secretary of State to set out in regulations further details around statements of compliance, which may include provisions

requiring the manufacturer to take certain specified steps to determine compliance with the security requirements for the preparation of the statement of compliance, as well as provisions around the retention, publishing and making available of the document. The exercise of this power will be subject to a negative resolution.

65 Subsection (7) provides a power for the Secretary of State to state that a manufacturer has complied with the statement of compliance duty when certain conditions are met.

> Statement of compliance regulations
>
> The Secretary of State may set out in regulations the minimum time that records of compliance statements must be kept, and the steps a manufacturer must take to assure compliance.
>
> The Secretary of State may also establish in regulations that the above is not required if a product is accompanied by documentation confirming that the manufacturer has complied with another cyber security

regime, because the Secretary of State recognises these standards as equivalent or sufficient to meet the intentions of this regime.

Clause 10: Duty to investigate potential compliance failures

66 Subsection (2) sets out a requirement for manufacturers to take all reasonable steps to investigate a compliance failure in relation to a product if they are informed that there is, or may be, a compliance failure relating to a product and if they are aware or ought to be aware that the product is or will be a UK consumer connectable product as defined in clause 54.

Example: a third party identifies a compliance failure

A security researcher discovers a specific software bug which makes the product default to a basic password setting after updating and notifies the manufacturer. The manufacturer must

then investigate to determine if this constitutes a compliance failure.

Example: a manufacture identifies a compliance failure

A manufacturer makes products available in the UK and several other countries as well. The manufacturer is aware of reports in another country that their product has a vulnerability which means they may not be complying with security requirements in relation to identical products made available to customers in the UK. They then have a duty to investigate if the products in the UK are impacted and if this constitutes a compliance failure.

67 The obligation to investigate reports of compliance failures applies at any time after a product has been made available in the United Kingdom.

Clause 11: Duties to take action in relation to compliance failure

68 This clause provides that, if a

manufacturer is aware, or ought to be aware, of a compliance failure as defined in clause 11(9) and is aware, or ought to be aware, that product is or will be a UK consumer connectable product as defined in clause 54, then the manufacturer must take all reasonable steps to (a) prevent the product from being made available in the United Kingdom, and/or (b) remedy the compliance failure.

69 Subsections (3) and (4) require that the manufacturer is transparent about this process. The manufacturer must notify persons including the enforcement authority, any other manufacturer of the product of which the manufacturer is aware and any importer or distributor to whom the manufacturer supplied the product. When certain conditions are met in relation to a compliance failure, the manufacturer must also notify any customer to whom it directly supplied the product. These conditions will be set out in regulations by the Secretary of State using the power in

subsection (5).

70 Subsection (6) sets out that the notification under subsection (3) must include detail of (a) the compliance failure, (b) any risks of which the manufacturer is aware that are posed by the compliance failure, and (c) any steps taken by the manufacturer to remedy the compliance failure and whether or not those steps have been successful.

71 Subsections (7) and (8) ensure that relevant persons are not required to duplicate notifications made by others in the supply chain.

72 The duties in this clause apply at any time after a product has been made available in the United Kingdom.

Clause 12: Duty to maintain records

73 This clause requires manufacturers to keep records of compliance failures and investigations relating to products for which they are the manufacturer. Subsections (2) and (3) set out the information that needs to be

captured in this process. Records and information on compliance failures and investigations must be kept for a minimum of ten years. These records may be requested by the Secretary of State in the course of investigating and enforcing the legislation.

Clause 13: Duties to take action in relation to manufacturer's compliance failure

74 A manufacturer that is not established in the United Kingdom may authorise a person in the United Kingdom to perform certain duties on its behalf as described in clause 51 and to act as an "authorised representative". Clause 13 places a duty on any manufacturer's authorised representatives to notify the manufacturer and then also the enforcement authority if they are informed that there is or may be a compliance failure and if the authorised representative is aware or ought to be aware that the product is or will be a UK consumer connectable product as defined in clause 54.

75 This duty applies at any time after a product has been made available in the United Kingdom.

Clause 14: Duty to comply with security requirements

76 This clause places a duty on importers to comply with any relevant security requirements that apply to an importer. Compliance is required where one of two conditions is met. Subsection (2) sets out the first condition that the duty applies where the importer intends for, is aware that, or ought to be aware that the product will be a UK consumer connectable product, as defined in clause 54.

77 Subsection (3) sets out the second condition. It provides that the importer is also subject to this duty where a product has become a UK consumer connectable product, and at the time the importer made the product available, it intended, was aware, or ought to have been aware that the product would become one.

Clause 15: Statements of compliance

78 This clause provides that an importer may not make a product available in the United Kingdom unless it is accompanied by a statement of compliance, or summary statement, where the importer intends for, is aware that, or ought to be aware that the product will be a UK consumer connectable product, as defined in clause 54.

79 Subsection (3) provides a power for the Secretary of State to set out in regulations the period of time for which importers must retain a copy of statements of compliance. Subsection (4) provides that the Secretary of State may establish via regulations when an importer must make a statement of compliance or summary statement available. These will be subject to the negative resolution procedure.

80 Subsection (5) sets out that if a manufacturer satisfies the conditions set out in regulations made under clause 9(7), then importers do not have a duty to ensure a

statement of compliance or summary statement accompanies the product. Instead the importer must be satisfied that the manufacturer fully complies with any conditions specified in regulations made under clause 9(7).

Clause 16: Duty not to supply products where compliance failure by manufacturer

81 This clause provides that an importer must not make a relevant connectable product available in the United Kingdom if it knows or believes that there is a compliance failure and intends for, is aware or ought to be aware that the product will be a UK consumer connectable product as defined in clause 54. Subsection (2) defines ‘compliance failure’ as a failure by the manufacturer of a product to comply with security requirements relating to the product.

82 This applies, for example, when the importer is informed (or could reasonably have been made aware by third parties including the

press, regulators or security experts) that the manufacturer has not or is unlikely to have complied with relevant security requirements.

Clause 17: Duty to investigate potential compliance failures of importer or manufacturer

83 This clause sets out a requirement for importers to take all reasonable steps to investigate any compliance failure, if they are informed that there is, or may be, a compliance failure and the product is or will be a UK consumer connectable product, as defined in clause 54. An importer may, for example, become informed of a compliance failure because information is circulating in the public domain or a third party provides information directly to it. A compliance failure may be by either the importer or a manufacturer.

84 The obligation to investigate potential compliance failures applies at any time after a product has been made available in the United Kingdom.

Clause 18: Duties to take action in relation to importer's compliance failure

85 This clause provides that, if an importer is aware, or ought to be aware, of a compliance failure by the importer as defined in clause 18(7) and is aware or ought to be aware that the product is a UK consumer connectable product as defined in clause 54, it must take all reasonable steps as soon as is practicable to remedy the compliance failure.

86 Subsections (3) and (4) require that the importer notifies relevant parties as soon as possible of a compliance failure. When certain conditions are met in relation to a compliance failure, the importer must notify any customer to whom it directly supplied the product. These conditions will be set out in regulations by the Secretary of State using the power in subsection (5) and will be subject to the negative resolution procedure.

87 Subsection (6) sets out that the notification under subsection (3) must include (a) details of

the compliance failure, (b) any risks of which the importer is aware that are posed by the compliance failure, and (c) any steps taken by the importer to remedy the compliance failure and whether or not those steps have been successful.

88 The duties in this clause apply at any time after a product has been made available by an importer to a customer in the United Kingdom.

Clause 19: Duties to take action in relation to manufacturer's compliance failure

89 If an importer becomes aware, or ought to be aware, of a manufacturer's compliance failure and is aware, or ought to be aware, that a product will be a UK consumer connectable product, then it has a duty to act. The importer must contact the manufacturer about the compliance failure as soon as possible, and, if it appears that the compliance failure is not going to be remedied, then subsection (4) requires the importer to take all reasonable steps as soon as is practicable to prevent the

product from being made available to customers in the UK.

90 Subsection (5) requires the importer to notify certain persons of the compliance failure after contacting, or attempting to contact the manufacturer. These persons are specified in subsection (6), and include the enforcement authority and any distributor to whom the importer has supplied the product. The importer may also need to notify any customer to whom it directly supplied the product. The conditions for notifying customers will be set out in regulations by the Secretary of State using the power in subsection (7) and will be subject to the negative resolution procedure.

91 Subsection (8) sets out that notifications under subsection (5) must include (a) details of the compliance failure, (b) any risks of which the importer is aware posed by that compliance failure, and (c) any steps of which the importer is aware that the manufacturer has taken to remedy the failure and if those steps have been successful.

92 Subsection (9) sets out that when an importer notifies a distributor to whom it has supplied a product of a compliance failure, the importer must also inform the distributor if the manufacturer is aware of the compliance failure and if the enforcement authority has been notified of the compliance failure.

93 Subsection (10) ensures that relevant persons are not required to duplicate notifications made by others in the supply chain.

94 The duties in this clause apply at any time after an importer of a product has made it available in the United Kingdom.

Clause 20: Duty to maintain records of investigations

95 This clause requires importers to keep records of any investigations into compliance failures or suspected compliance failures, as defined in subsection (5), relating to products for which they are an importer. These records will allow a clear audit of the importer's

activities and help investigations into compliance failures. Subsection (2) and sets out the minimum content that needs to be captured in this process. Subsection (3) ensures that the importer will not breach its record keeping duty due to the actions of the manufacturer but the importer must have taken reasonable steps to obtain all required information from the manufacturer. Records and information on compliance failures and investigations must be kept to a minimum of ten years.

Clause 21: Duty to comply with security requirements

96 This clause places a duty on distributors to comply with any relevant security requirements relating to a relevant connectable product. Compliance is required if one of two conditions is met. Condition one is met if the distributor intends for, is aware that, or ought to be aware that the product will be a UK consumer connectable product, as defined in clause 54.

97 Condition two is met where a product has become a UK consumer connectable product, as defined in clause 54, and at the time the distributor made the product available, it intended, was aware, or ought to have been aware that the product would become a UK consumer connectable product.

Clause 22: Statements of compliance

98 This clause provides that a distributor of a relevant connectable product may not make a product available in the United Kingdom unless it is accompanied by a statement of

compliance, or a summary of the statement of compliance. This duty applies if the distributor intends for the product to be a UK consumer connectable product as defined in clause 54 or is aware or ought to be aware that the product will be a UK consumer connectable product.

99 Subsection (3) sets out that if a manufacturer satisfies the conditions set out in regulations made under clause 9(7), then distributors do not need to ensure the presence of a statement of compliance or summary statement of compliance, so long as the distributor is satisfied that the manufacturer is fully compliant with the conditions set out in regulations made under clause 9(7).

Clause 23: Duty not to supply products where compliance failure by manufacturer

100 A distributor must not make the product available in the United Kingdom if it knows or believes there is a compliance failure in relation to that product and intends for the product to be or is aware or ought to be aware

that the product will be a UK consumer connectable product, as defined in clause 54. For the purposes of this clause, “compliance failure” is defined in subsection (2) as a failure by a manufacturer of the product with relevant security requirements relating to that product.

Clause 24: Duties to take action in relation to distributor’s compliance failure

101 This clause provides that, if a distributor becomes aware, or ought to be aware, of a compliance failure in relation to a product as defined in subsection (7) and is aware or ought to be aware that the product will be a UK consumer connectable product , it must (a) as soon as is practicable, take all reasonable steps to remedy the compliance failure, and (b) notify the enforcement authority and in certain circumstances the customer. Subsection (5) provides for the Secretary of State to set out in regulations the conditions for when the customer must be notified of a compliance failure.

102 Subsection (6) sets out that notifications under subsection (3) must include (a) details of the compliance failure, (b) any risks of which the distributor is aware posed by that compliance failure, and (c) any steps taken by the distributor to remedy the compliance failure and whether or not those steps have been successful.

103 The duties in this clause apply at any time after a product has been made available by a distributor to a customer in the United Kingdom.

Clause 25: Duties to take action in relation to manufacturer's compliance failure

104 This clause provides that, if a distributor of a relevant connectable product becomes aware, or ought to be aware, of a manufacturer's compliance failure, as defined in subsection (2) and is aware or ought to be aware that the product will be a UK consumer connectable product as defined in clause 54, then the distributor has a duty to act.

105 Subsection (3) requires that the distributor to contact the manufacturer about the compliance failure as soon as possible.

106 Subsection (4) provides that, if it is not possible to notify the manufacturer and a relevant person other than the manufacturer supplied the product to the distributor, the distributor must contact that other relevant person about the compliance failure as soon as possible.

107 If it appears that the compliance failure is not going to be remedied by the manufacturer in accordance with clause 11(2)(b), the distributor must take all reasonable steps to prevent the product from being made available to customers in the United Kingdom.

108 The distributor must also notify the persons in subsection (7) of the compliance failure as soon as possible, after it has contacted (or attempted to contact) the manufacturer. When certain conditions are met in relation to a compliance failure, the

distributor must also notify any customer to whom it directly supplied the product. These conditions will be set out in regulations by the Secretary of State using the power in subsection (8).

109 Subsection (9) sets out that any such notification must include (a) details of the compliance failure, (b) any risks of which the distributor is aware posed by that compliance failure, and (c) any steps which the manufacturer has taken to remedy the failure of which the distributor is aware and whether or not those steps have been successful.

110 Subsection (10) sets out that where the distributor notifies a distributor or an importer to whom it has supplied a product or the person from whom they obtained the product of a compliance failure, the distributor must also inform them whether the manufacturer is aware of the compliance failure and weather the enforcement authority has been notified of the compliance failure.

111 Subsection (11) ensures that relevant persons are not required to duplicate notifications made by others in the supply chain.

112 The duties in this clause apply at any time after a distributor of a product has made it available in the United Kingdom.

Chapter 3: Enforcement

Clause 26: Enforcement of Part 1

Subsection (1) establishes that the Secretary of State will be responsible for enforcing the provisions of Part 1 and any regulations made under it.

113 Subsections (2) and (3) set out that the powers of investigation in Schedule 5 to the Consumer Rights Act 2015 are available to the Secretary of State and amend Schedule 5 of the Consumer Rights Act 2015 to that effect.

114 Subsection (4) removes the restriction in paragraph 13(4) of Schedule 5 of the Consumer Rights Act 2015 that limits information requests to determining if a breach has occurred and allows the Secretary of State to exercise powers in relation to production of information for any purpose relating to the enforcement of Part 1. This provides for the Secretary of State to request relevant information both to determine that a breach has occurred and to ensure that penalties are correctly applied. For instance, requests for

financial information might be needed to ensure only relevant entities are used when calculating worldwide revenue for a company group.

115 Subsection (4) also removes the restriction in paragraph 13(5) of Schedule 5 to the 2015 Act, so that the Secretary of State can request that a manufacturer, distributor or importer produce information without there needing to be a reasonable suspicion of a breach of the legislation. This allows the Secretary of State to undertake their enforcement functions. Requesting information is needed to correctly ascertain if compliance failures have occurred, the level of risk arising from these compliance failures and ensure notices or corrective measures are issued where it is deemed necessary and proportionate to do so.

116 Subsection (5) provides that the Secretary of State may not bring proceedings for offences under Part 1 in Scotland, to ensure that the legislation does not contradict Scottish court procedures.

Clause 27: Delegation of enforcement functions

117 This clause provides for the Secretary of State to enter into an agreement with any person authorising that person to exercise any enforcement function of the Secretary of State. Subsection (3) provides that the Secretary of State may cancel an agreement for the undertaking of enforcement functions at any time. An agreement with another person to exercise enforcement functions does not prevent the Secretary of State from also performing a function to which the agreement relates.

118 Subsection (2) provides that the Secretary of State may make payments for the performance of enforcement functions to an authorised person. This could be payment for singular enforcement actions or continuous responsibility for multiple enforcement activities.

119 Subsection (5) defines an “enforcement function” as (a) any function of the Secretary of State under this Chapter, or (b) any function of

the Secretary of State under Schedule 5 to the Consumer Rights Act 2015, so far as exercisable for the purposes of this Part.

120 Where a person is authorised to undertake an enforcement function under subsection (1), subsection (6) provides that any reference to the Secretary of State in provisions relating to that enforcement function should also be read as a reference to that person.

121 This is a routine power that replicates other legislation such as Section 125 of the Environmental Protection Act 1990.

Clause 28: Compliance notices

122 This clause provides that the Secretary of State may give a compliance notice where they have reasonable grounds to believe a person has failed to comply with a relevant duty.

123 Subsection (2) describes a compliance notice as a notice requiring the recipient to comply with a relevant duty within a specified time frame. Subsection (3) provides that a

compliance notice must (a) set out the reasons for giving the compliance notice, (b) explain what may happen if the person does not comply with it, and (c) explain how the person may appeal against it.

124 Subsection (4) provides that a compliance notice may require the recipient to take specified steps to comply with a relevant duty and/or to provide evidence to satisfy the Secretary of State within a specified period that the person has complied or is complying with the relevant duty.

125 Subsection (5) requires that, before issuing a compliance notice, the Secretary of State must notify the recipient that they intend to give a compliance notice and provide an opportunity for the recipient to make representations about the giving of the notice.

126 Subsection (6) sets out that the Secretary of State must not impose the compliance notice until 10 days after they have notified the recipient that they intend to issue a compliance

notice.

127 Subsection (7) provides that only one compliance notice can be given for the same act or omission. A person may receive multiple notices where there are repeated and different breaches.

Clause 29: Stop notices

128 This clause provides that the Secretary of State may give a stop notice n where they have reasonable grounds to believe that a person is carrying on, or is likely to carry on, an activity in breach of a relevant duty.

129 Subsection (2) describes a stop notice as a notice requiring the recipient to stop carrying on an activity within a specified time frame. Subsection (3) provides that a stop notice must (a) set out the reasons for giving the stop notice, (b) explain what may happen if the person does not comply with it, and (c) explain how the person may appeal against it.

130 Subsection (4) provides further detail as to what a stop notice may require, including

informing customers of risks posed by the product to which the stop notice relates.

131 Subsection (5) provides that, before issuing a stop notice, the Secretary of State must notify the recipient that they intend to give a stop notice and provide an opportunity for the recipient to make representations about the giving of a notice.

132 Subsection (6) provides that the Secretary of State must not impose the stop notice until 10 days after they have notified the recipient that they intend to issue a stop notice.

133 Subsection (7) provides that, if the Secretary of State considers that there is an urgent need to give a stop notice, then the requirements in subsections (5) and (6) do not apply.

Clause 30: Recall notices

134 This clause provides a power for the Secretary of State to give a recall notice to a manufacturer or its authorised representative, an importer or a distributor.

135 Subsection (1) provides that a recall notice may only be given if (a) the Secretary of State has reasonable grounds to believe that there is a compliance failure in relation to any UK consumer connectable products that have been supplied to customers, (b) the Secretary of State considers that the action (if any) being taken by any relevant person in relation to the compliance failure is inadequate, and (c) the Secretary of State considers that any no other action which the Secretary of State may take under clauses 28, 29 and 42 would be sufficient to deal with the risks posed by the compliance failure.

136 Subsection (3) describes a recall notice as a notice requiring the recipient to make arrangements within a specified period for the return of the products to the recipient or to another person specified in the notice.

137 Subsection (4) provides that a stop notice must (a) set out the reasons for giving the recall notice, (b) explain what may happen if the person does not comply with it, and (c)

explain how the person may appeal against it.

138 Subsection (5) provides some further detail as to what a recall notice may require, including, informing customers of risks posed by the product to which the recall notice relates.

139 Subsection (6) provides that before issuing a recall notice, the Secretary of State must notify the recipient that they intend to give a recall notice and provide an opportunity for the recipient to make representations about the giving of a notice.

140 The Secretary of State must not impose a recall notice until 10 days after they have notified the recipient that they intend to issue a recall notice.

141 Subsection (8) provides that if there is an urgent need to give a recall notice, then the requirements in subsections (6) and (7) do not apply.

Example of issuing a recall notice

A smart camera with a universal default password is hacked and used to spy on consumers or to facilitate robberies.The manufacturer is unable and unwilling to comply with its duties in relation to the product and continues to supply the product to customers. After assessing the risk of the breach, the Secretary of State determines the compliance failure poses an immediate and high risk to any UK household which has purchased this product and to the UK's economy due to the products facilitation of robberies.

The Secretary of State gives a recall notice to the manufacturer/importer/distributor(s) or to any combination of relevant persons involved in the supply chain of the product to ensure the products are removed from circulation and the threat is eliminated.

Clause 31: Power to vary or revoke enforcement notices

142 This clause provides the Secretary of State with power to vary or revoke an enforcement notice, as long as the changes do not make the notice more onerous than the original notice.

> Example of varying a stop notice
>
> The enforcement authority identifies that a popular baby monitor comes with a default password. The enforcement authority issues a compliance notice to the manufacturer, requiring that they ensure the product complies with all technical aspects of a security requirement within 14 days or stop making it available. The manufacturer has identified a solution to the problem and requests the Secretary of State allows the manufacturer 28 days to comply with the notice instead. The additional time is requested because another manufacturer supplies a key component part within the product and the primary manufacturer needs to

work with its supplier to achieve compliance.

The Secretary of State is satisfied that the manufacturer is taking reasonable steps to comply, the additional time is genuinely needed, and that the extension does not materially expose citizens, networks and infrastructure to additional harm. The Secretary of State decides to vary the notice so that compliance is required within 28 days.

Example of revoking a stop notice

The Secretary of State issues a stop notice requiring a distributor to stop selling a non-compliant smart television within 60 days. The distributor works with the manufacturer to resolve the compliance failure and within 15 days the product complies with the security requirements. The Secretary of State is satisfied that the product complies, and decides to revoke the notice so the distributor can continue to make it available.

Clause 32: Failure to comply with enforcement notice

143 This clause makes it an offence for a recipient of an enforcement notice to fail to comply with that notice. A person guilty of an offence under this clause is liable to a fine of the type set out in subsection (9).

144 Subsections (2) sets out a defence to this offence for the recipient of the notice to show that they took all reasonable steps to comply with the notice. Subsection (3) provides that a person is taken to have shown that fact where sufficient evidence is adduced to raise this as an issue and the contrary is not proven beyond reasonable doubt. When considering the defence, the relevant courts will consider evidence provided to show the recipient's effort to comply with the notice as well as any evidence demonstrating the recipient could have undertaken additional effort to comply with the notice.

145 The recipient of the enforcement notice is

responsible for complying with it and accountable for any failure to comply with the notice. This is true even if the recipient has not made themselves available for correspondence with the Secretary of State and failed to receive correspondence sent to an appropriate address.

146 A person charged with an offence under this clause must serve a notice on a prosecutor or obtain the permission of the court if that person intends to rely on a defence under subsection (2), which involves a third party allegation. 'Third party allegation' is defined in subsection (5) to mean the act or omission of another person or reliance on information provided by another person.

147 Subsection (7) states that in England, Wales or Northern Ireland the prosecutor must be notified 7 days in advance of the hearing of the proceedings and subsection (8) states that in Scotland the prosecutor must be notified 10 days before the trial diet or where there is an intermediate diet, at or before this diet.

Clause 33: Appeals against enforcement notices

148 Subsection (1) provides that a recipient of an enforcement notice will be able to appeal to the First-tier Tribunal against the notice or any provision of it, including the decision to issue it. Appeals can also be made against any variation to a notice made under clause 31.

149 Appeals must be made within 28 days from the date the notice was given by the enforcement authority. If the appeal is against the variation of the notice, then the appeal must be within 28 days beginning on the day on which the notice was varied.

150 Subsection (3) establishes the Tribunal's power to either confirm the notice or, if it is satisfied that any of the grounds in subsection (4) apply, to vary or cancel the notice.

151 Subsection (5) provides that if the Tribunal cancels a notice (whether in part or in full), it may require the person who gave the notice to reconsider the matter and make a new decision in accordance with the Tribunal's

ruling.

152 Subsection (6) limits the Tribunal's powers so that the Tribunal cannot direct the person who gave the notice to take any action that they would otherwise be unauthorised to take. The Tribunal cannot, for example, order a person to recall products that are not in scope of Part 1 of this Bill, because this exceeds the powers of the Secretary of State.

153 Subsection (7) allows the Tribunal to review the facts on which the decision to give the notice, or to include any provision of it, was based. The Tribunal may also consider evidence that was not available to the person who issued the notice. This allows for an appeals process even where the person who received the notice did not have an opportunity to submit evidence to the enforcement authority prior to the service of the notice by virtue of clause 29(7) or clause 30(8).

154 Subsections (8) and (9) act as safeguards. Subsection (8) temporarily suspends the effect

of the enforcement notice, or the variation of the enforcement notice, against which an appeal is made until that appeal is determined or withdrawn. Subsection (9) allows the Upper Tribunal to suspend the notice, or any part of it, if an appeal against the decision of the First-tier Tribunal is or may be made until the Upper Tribunal determines that appeal or until it is withdrawn.

Clause 34: Compensation for notices wrongly given

155 This clause sets out that the Secretary of State is liable to pay compensation to the person on whom a stop or a recall notice is wrongly given for loss or damage caused as a result of the giving of the notice. Compensation is only payable if the breach that led to the imposition of the stop or recall notice did not occur, and the decision to give a notice was not due to any neglect or default by the recipient of the notice.

156 Subsection (3) states that the Secretary of

State will be responsible for determining the amount of compensation payable to a person under this clause.

157 Subsection (4) and (5) states that the Secretary of State may take into consideration the extent to which the person took reasonable steps to reduce the loss or damage caused as a result of the giving of the notice.

158 Subsection (6) states that a person seeking compensation must make a claim to the Secretary of State which includes evidence of the loss or damage in respect of which compensation is sought and the amount of the compensation sought. The claim must be made in a form and manner directed by the Secretary of State.

159 Subsection (7) provides that the Secretary of State must decide whether compensation will be paid and the amount of any compensation (if payable) and notify the person making the claim of their decision within 45 days beginning on the day on which

the Secretary of State receives a claim.

Clause 35: Appeals against decisions under section 34

160 This clause sets out a person's right to appeal to the First-tier Tribunal against the decision not to award compensation or against the amount of the compensation payable under clause 34.

161 An appeal should be made within 28 days beginning on the day the Secretary of State notified the person claiming compensation whether compensation would be paid, or the amount to be paid (if payable).

162 Where the decision appealed against is the decision not to award compensation, subsections (3) and (4) give the Tribunal the power to confirm or quash the decision that is appealed and where it is quashed, to order the Secretary of State to pay compensation of an amount determined by the Tribunal or refer the decision back to the Secretary of State to retake the decision in accordance with its

ruling.

163 Where the decision appealed against is the amount of compensation awarded, subsection (5) provides that the Tribunal may confirm the amount of compensation awarded, vary the amount of the compensation or require the Secretary of State to retake the decision that is appealed in accordance with its ruling.

164 Subsection (6) provides that an appeal against the decision not to award compensation or against the amount of the compensation may be made on the grounds that the decision appealed against was based wholly or partly on an error of fact or that the decision appealed against was wrong in law. Appeals against the amount of the compensation may also be made on the ground that the amount of the compensation was unfair or unreasonable for any other reason.

165 Subsection (7) provides that the Tribunal

may review any facts on which the decision to appeal was based and take into account evidence not available to the Secretary of State and subsection (8) provides that the Tribunal cannot direct the Secretary of State to pay any compensation that they would not be otherwise be liable to pay under clause 34(2).

Clause 36: Monetary Penalties

166 This clause provides that, where a person has, on the balance of probabilities, failed to comply with a relevant duty, the Secretary of State may give a penalty notice requiring the recipient to pay a fine of a specified amount within a specified time period of no less than 28 days. The amount must not exceed any maximum established under clause 38.

167 A penalty may be issued even if the recipient has not previously received an enforcement notice in respect of the relevant breach but a person may not receive more than one penalty notice for a single breach. All penalties paid to the Secretary of State are to be paid into the Consolidated fund.

168 Where a breach continues beyond the period set in the penalty notice, subsection (5) provides that a daily penalty can be imposed requiring the person to pay up to £20,000 for each additional day a breach takes place. There is no cap on the potential penalty accrued in daily penalties. If a daily penalty is to be imposed, then the daily penalty amount must also be set out in the initial penalty notice.

Clause 37: Determining the amount of a penalty

169 This clause sets out that the penalty must be an amount considered by the Secretary of State to be appropriate and proportionate to the breach for which it is imposed. It must be determined taking into account the effects arising from a breach, and action taken by the recipient to remedy the breach or mitigate its effects.

Clause 38: The relevant maximum

170 This clause sets the relevant maximum penalty for breaches to be the greater of £10

million or 4 per cent of the person's qualifying worldwide revenue for the person's most recent complete accounting period.

171 Where a non-compliant relevant person is a member of one or more groups (e.g. groups of companies), subsection (6) provides a power for the Secretary of State to determine the class of members within the group or groups that will have their revenue taken into account for the purposes of calculating the relevant maximum penalty.

172 Subsection (7) provides a power for the Secretary of State to set out in regulations how qualifying worldwide revenue for a period is to be determined for the purpose of calculating the maximum possible penalty.

173 Regulations under these powers will be subject to the affirmative resolution procedure.

Clause 39: Penalty notices: further provision

174 This clause sets out that, before giving a penalty notice, the Secretary of State must notify the recipient of their intention to give a

notice and provide an opportunity for the recipient to make representations. Although there is no formal time limit within which a relevant person has to make representations, in practice it is likely that a relevant person would make representations within 28 days as the Secretary of State can issue a penalty notice as soon as 28 days after notification.

175 Subsection (3) sets out that the penalty notice must (a) give reasons for the notice, (b) include the amount of the penalty, (c) set out how payment may be made,(d) the deadline for making payment, (e) explain how the notice can be appealed, and (f) explain the consequences of failing to pay the penalty.

176 Subsections (4) and (5) provide that after issuing a variable monetary penalty notice, the Secretary of State may vary or revoke the notice but any variation may not make the notice more onerous. For example, the Secretary of State may reduce the amount of the penalty or allow for it to be paid at a later date but cannot require a higher penalty to be

paid after the initial penalty notice has been issued.

Clause 40: Enforcement of penalty notices

177 This clause establishes the procedure for enforcing a penalty notice in England and Wales, Scotland, and Northern Ireland.

Clause 41: Appeals against penalty notices

178 This clause provides that a person who receives a penalty notice has the right to appeal to the First-tier Tribunal against the imposition of a penalty, the amount of a penalty or period in which a penalty or any part of it must be paid. Any appeal must be brought before the end of the period of 28 days beginning with the day on which the penalty notice was given, or the day on which the penalty notice was varied by the Secretary of State.

179 Subsections (3), (4) and (5) set out what the Tribunal may do, and the conditions under which the Tribunal may cancel or vary the decision of the Secretary of State.

180 Where the Tribunal cancels the notice, it may refer the matter back to the decision-maker with a direction to reconsider the matter and make a new decision in line with its ruling. However, the Tribunal may not direct the person who gave the penalty notice to take any action that the person would not have otherwise have the power to take.

181 Subsection (7) provides that the Tribunal may review any determination of fact on which the decision appealed against was based. The Tribunal may also take into account evidence that was not available to the person who gave the notice.

182 Subsection (8) is a safeguard that ensures that the penalty notice will not have effect (and therefore a penalty will not be payable) if an appeal against it is made to the First-tier Tribunal until that appeal is determined or withdrawn. The same applies in respect of a variation of a penalty notice. Subsection (9) is similar and it allows the Upper Tribunal, if an appeal against the decision of the First-tier

Tribunal is or may be made, to suspend the penalty notice until the appeal is determined or withdrawn.

Clause 42: Forfeiture

183 This clause sets out when relevant connectable products may be forfeited.

184 "Forfeitable products" are defined to include relevant connectable products that are in the possession or control of specific economic operators. This includes products that have been returned, for example, as a result of a recall notice, to one of the aforementioned economic operators. Products detained under paragraph 28 of Schedule 5 to the Consumer Rights Act 2015 are also included.

185 Subsections (2) and (3) provide the conditions under which the Secretary of State may apply to court for an order for the forfeiture of products and the conditions upon which the court may make an order for the forfeiture of products.

186 Subsection (6) provides for the court to order the delivery of property to the Secretary of State, or such other person as the court may direct. It also provides for the Secretary of State, or such other person as the court may direct, to destroy or otherwise dispose of the property in whatever way the Secretary of State or other person considers appropriate. An order under this clause may require the property to be destroyed or otherwise disposed of in accordance with any directions of the court.

187 Subsections (7),(8), and (9) provide for the conditions under which forfeited products detained under paragraph 28 of Schedule 5 to the 2015 Act are returned to whomever is entitled to them.

Clause 43: Further provision about forfeiture

188 This clause sets out how applications for an order for the forfeiture of products will be made to a the court in England and Wales and Northern Ireland.

189 Applications for an order for forfeiture of products can be made in cases where proceedings have been brought in England and Wales and Northern Ireland for an offence under either (a) Clause 32 or (b) paragraph 36(1) or (2) of Schedule 5 to the 2015 Act.

190 Subsection (4) establishes that the court may only issue a forfeiture if (a) the Secretary of State has given notice to every identifiable person with an interest in the product of the application, date and location of the proceedings for forfeiture, or (b) the court is satisfied that it was reasonable in the circumstances not to have given such notice.

191 Subsection (5) provides for any person having an interest in any forfeitable products to appear in court proceedings under clause 42.

192 Subsection (6) is a safeguard. It provides that a forfeiture order may not take effect until the period for appealing against the court's decision to order forfeiture has ended or if an appeal is made, until it has been determined or withdrawn.

Clause 44: Appeal against decision under section 42

193 This clause sets out that appeals against an order for the forfeiture of products under clause 42 are permitted by any party to the proceedings in which the order was made, and any other parties entitled to the products.

194 Subsection (2) provides for the Secretary of State to appeal against a decision not to make an order for forfeiture under clause 42, or an order under subsection (8) of that clause for the return of any products.

195 Subsection (5) provides that an appeal under this clause must be brought before the end of the period of 28 days, beginning with the date of the order or other decision

appealed against.

Clause 45: Power to inform public about compliance failures

196 This clause provides a power for the Secretary of State to publish whatever information they consider appropriate in order to inform the public about (2)(a) the nature of the compliance failure, (b) any risks posed by using the product, or (c) any steps that may be taken to mitigate the effect of any such risks, where the Secretary of State has reasonable grounds to believe there is a compliance failure. This power is subject to any enactment or rule of law restricting the disclosure of information.

Clause 46: Power to publish details of enforcement action taken against relevant persons

197 This clause enables the Secretary of State to publish information about failures by relevant persons to comply with their security requirements. The power also allows the Secretary of State to publish details about

enforcement notices, penalties and forfeiture orders.

Clause 47: Power to recall products

198 This clause provides a power for the Secretary of State to recall non-compliant products that have been supplied to customers in cases where a recall notice has not been complied with or where it was not possible to give a recall notice to the relevant person, and the Secretary of State has reasonable grounds to believe that there is a compliance failure in consumer connectable products supplied to consumers.

199 Subsection (4) provides that the Secretary of State may make arrangements for the delivery, disposal and destruction of the recalled products.

200 Subsection (5) provides that the Secretary of State may pay any amount it considers appropriate to customers who return products in a recall organised by the Secretary of State.

201 Subsection (6) provides that if the

Secretary of State provides any financial incentive for the return of the product organised under clause 46 to a customer, a relevant person who is required to pay compensation to that customer will be able to deduct the amount paid by the Secretary of State from any amount that the relevant person is required to pay (whether as a result of the exercise of the customer's statutory rights or otherwise).

202 Subsection (7) provides that, where the recipient of a recall notice fails to comply with it, the Secretary of State may recover any costs or expenses reasonably incurred in taking action under this clause relating to a compliance failure from the person who failed to comply with the recall notice.

Clause 48: Disclosure of information

203 This clause allows the Secretary of State to disclose to a person any information obtained in connection with, where the disclosure made is for a purpose connected with an enforcement function of the Secretary

of State. Subsection (2) provides that a person may disclose any information to the Secretary of State if it is for the purposes of enabling or assisting the Secretary of State to exercise any enforcement function.

204 As per subsection (3), this can be done without breaching any restriction on the disclosure of information imposed on the person making the disclosure. However, subsections (4) and (5) provide that any action taken under this clause must not contravene data protection legislation or any of Parts 1 to 7 or Chapter 1 of Part 9 of the Investigatory Powers Act 2016.

205 Subsection (7) inserts Part 1 of the Product Security and Telecommunications Act 2021 into Schedule 14 of the Enterprise Act 2002 to empower the Secretary of State to disclose information to others (e.g. other regulators) so that they can carry out their functions pursuant to any act listed in Schedule 15 to the 2002 Act, or any subordinate legislation as may be specified for

the purposes of this section 241(3) of the 2002 Act.

Clause 49: Offence of purporting to act as authorised to exercise enforcement function

206 This offence is in addition to the offence of purporting to act as officer at paragraph 37 of Schedule 5 to the Consumer Rights Act 2015.

207 Whilst paragraph 37 of Schedule 5 to the 2015 Act provides that it is an offence for a person who is not an officer of an enforcer to purport to act as such under Part 3 or 4 of that Schedule, this clause additionally sets out that it is an offence for a person to purport to act as authorised to exercise a function of the Secretary of State under Chapter 3 (the enforcement provisions).

208 Subsection (2) provides the maximum penalty that the relevant court can impose on a person found guilty of the offence.

Clause 50: Means of giving notices

209 This clause provides the means by which an enforcement notice can be given to a

person, namely (a) handing it to the person, (b) leaving it at the person's proper address, (c) sending it by post to the person at that address, or (d) where appropriate, sending it to the person by electronic means.

Clause 51: Liability of authorised representatives

210 Where a manufacturer established abroad authorises a person in the United Kingdom, with the agreement of that person, to perform any of the duties listed in subsection (3) on their behalf, this clause sets out that the authorised representative must comply with those duties. Subsection (5) stipulates that this does not affect the manufacturer's liability for a failure to comply with a duty.

Clause 52: Offences by directors, partners etc

211 This clause provides for the liability of a director, manager, secretary, or other similar officer of a corporate body, or any person purporting to act in such a capacity. This includes anyone in a similar corporate position, including members who manage the body

corporate's affairs, and partners of a Scottish partnership or those purporting to act as such a partner.

212 Such persons (as well as the body corporate) are liable when an offence is committed either with their consent or connivance or due to their neglect.

Chapter 4: Supplementary provision

Clause 53: Guidance

213 This clause provides the Secretary of State with the power to issue guidance on the effect of any provision made by or under Part 1 of the Bill

214 Subsection (2) provides the enforcement authority, as defined in clause 56, with a power to issue guidance on the exercise of any of its enforcement functions.

> Example of guidance supporting the enforcement function
>
> The Secretary of State publishes guidance for economic actors on how to engage with the enforcement

process and what parties should do upon receipt of a compliance notice. The guidance may include information on how the party should provide evidence of compliance or how the party can request that the notice is varied to allow a longer period of time to comply with the requirements of the notice..

Clause 54: Meaning of "UK consumer connectable product"

215 This clause defines the meaning of "UK consumer connectable products". They are defined as relevant connectable products that meet either of the conditions within subsection (2) or subsection (3)

216 Subsection (2) sets out the first condition - condition A. Condition A captures relevant connectable products that are or have been made available to UK consumers and that are not "used" at the point at which they are made available to customers.

217 Subsection (3) sets out the second condition - condition B. Condition B captures relevant connectable products that are or have been made available to businesses, where the products are not “used” at the point at which they are made available to customers and where products identical to it meet Condition A. Unused products that are made available to any UK customer, where other products in that product line have been, or are being made available to UK customers, will meet Condition B.

218 Duties predicated on a relevant person’s intent or knowledge that a relevant connectable product is or will be a “UK consumer connectable product” will cease to apply if a product that has previously been supplied to a customer is made available to UK customers again. This applies principally to products in a “used” condition (i.e. they have been “supplied” before). This clause also provides that duties continue to apply in relation to returned or reconditioned (when

reconditioned by or on behalf of the manufacturer as per the provisions in subsections (8) and (9)) products.

219 Subsection (10) provides a power for the Secretary of State to make regulations to repeal the conditions in subsections (2) and (3) which prevent duties from applying to used products and to amend any provisions of the product security part of the Bill that are necessary or appropriate consequent to the repeal of subsections (2)(b) and (3)(b). Regulations made in the exercise of this power will be subject to the affirmative resolution procedure by virtue of subsection 11.

Example of when a product sold to businesses may also be a "UK consumer connectable product":

A product may meet the definition of "UK consumer connectable product" even if it is solely aimed at business customers. A smart camera is advertised to business users but not to consumers in the UK because the distributor selling the camera only sells to businesses. However,

products identical to it (e.g. a smart camera of the same make and model) has been advertised (made available) to consumers in the UK by another distributor. This means the product should also be considered a “UK consumer connectable product” and must meet Part 1 security requirements, the distributor must also meet all relevant duties under Part 1.

As with condition A, if this camera has been supplied to customers (this means end users who can be either consumers or business users) before being advertised (made available to consumers in the UK), the camera will not be a consumer connectable product. The presumption is that products that have been supplied to users would have been used and used products are out of scope.

Intention

This ensures that all products that may reasonably be expected to be used by consumers are subject to the same security requirements, even where a particular individual product has not been directly made available

to consumers.

Clause 55: Meaning of "supply"

220 This clause defines the term "supply" for the purposes of Part 1.

221 Subsection (2) defines "supply" as supplying a product in the course of business. This includes 'supply' of a product by companies, sole traders, not for profit organisations and public bodies, but not supplies made by individuals acting outside the individual's business.

222 Subsection (2) also provides that supply is not limited to instances where a product is sold as part of a financial transaction. Provision of a product in exchange for non-monetary consideration (e.g. in exchange for goods or services, or as a gift accompanying a separate transaction) would also be considered a

"supply".

223 Subsection (3) provides that supply of a product does not include hiring out or the lending of a product unless the manufacturer is hiring out or lending the product, or unless the product is supplied under a hire-purchase agreement.

224 Subsection (4) provides that where a product has been supplied by being hired out or lent to a person, a continuation or renewal of the hire of loan or any transaction for the transfer after that time of any interest in the product to the person will not be considered as 'supply' of the product. This will ensure that administrative duties such as ensuring that there is a statement of compliance do not need to be complied with each time a person renews a rental agreement for a product because compliance at the first instance of 'supply' of the product to the same customer will be sufficient.

225 Subsection (5) provides that performance

of a contract for the carrying out of works that consist of or include the installation of a product into a building or structure will be treated as ‘supply’ for the purposes of Part 1, only in so far as it involves the provision of a product to a person by means of its installation into a building or a structure. The effect of this provision will be that customers will receive similar protections when hiring someone to install products in their premises as customers who directly buy in-scope products.

226 Subsection (6) provides that the provision of products by means of incorporating them in a building or a structure will be considered a supply of those products if they were incorporated in the course of a performance of a contract for the construction of the building or structure.

227 Subsection (7) provides that the transfer of in-scope products, either as fixtures or chattels, resulting from an agreement for the creation or a disposal of an interest in land, or resulting from the performance of such an

agreement, is not to be treated as a ‘supply’ of the products. However, an exception to this will be where the in-scope product is incorporated into or contained in a building, or part of the building, constructed on the land in question, the building or part of building is to be used for a particular purpose, and at the time of the supply the building or part of the building had not previously been used for that purpose.

228 The effect of subsection (7) is that a home owner selling their home (be it a flat or a house), or a business selling their premises with new in-scope products will not be considered distributors of those products. The distributor will be the retailer who sold the products to the property owner in the first instance, which is consistent with regular supply chains of UK consumer connectable products where a retailer is usually the distributor. However, for example, a developer selling, or otherwise disposing of an interest in a previously unoccupied house which includes in-scope products will be considered to have

supplied them to the new occupier.

229 Subsection (8) provides that selling a product for scrap does not constitute ’supply’. Subsection (9) provides that providing transport services for the purpose of enabling the supply of a product does not constitute ’supply’.

230 Subsection (10) provides that where a person (‘P’) who is the customer or the customer’s successor in title (e.g. a person who received the product as a gift by the original customer) returns the product temporarily (e.g. to a retailer for repairs under warranty) the subsequent return of the same product to ‘P’ (e.g. after the product has been repaired) is not a supply of that product. This provision ensures that persons merely providing repairs services will not be treated as distributors. However, if a product cannot be repaired and another product, even if it is of the same model, is provided to P as a replacement, this will be considered a new supply.

231 Subsection (11) distinguishes between retailers who supply products to customers (e.g. by selling the products) and companies that finance purchases of products (e.g. a financing company providing the funds to purchase a product). The effect of this provision is that retailers will be treated as distributors, but financial companies will not.

Example when consumer connectable products are "supplied"

A manufacturer rents out a smart camera (subsection (4)): A manufacturer rents out smart cameras to a consumer. The manufacturer will have to comply with the relevant duties when first renting out the product. Any subsequent renewals of the rental agreement with the same consumer will not require the manufacturer to comply with the duties again. Likewise, if the same consumer buys the product from the manufacturer after renting it, the manufacturer will not need to comply with the applicable duties again.

A developer equips a new house with built in smart products (subsection (5)): If a developer is hired to build a house with a built-in smart fridge, the developer will be considered a distributor with respect to that smart fridge, and will have to comply with the duties of distributors in clauses 21-25, e.g. not make the product available if there is a compliance failure and ensure that the product is accompanied by a

statement of compliance, etc.

This provision will not capture individuals installing commonly available to consumers products.

A builder is hired by a homeowner to build a garage fitted with smart surveillance cameras (subsection (6)): If a construction company is hired to build a garage and it installs a smart camera while building the garage, the company would be considered to have supplied that camera and as distributors, they would need to comply with the relevant duties.

A developer sells to a consumer a new building with smart appliances (subsection (7)): If a developer builds a new house with incorporated and freestanding smart products and appliances such as smart locks and microwaves, the developer will be considered a distributor of the products and appliances and will need to comply with the duties of distributor when selling the house to a consumer.

The developer will not need to comply

with the duties of a distributor if the house was previously occupied. Individuals selling a flat or house will not be considered distributors and will not need to comply with any duties arising from the sale.

This provision helps to capture smart home control systems within the scope of the legislation.

Instances where a product is not supplied because it is part of a wider transaction: If an electrician hired to repair a smart oven, installs a new smart thermostat, will not be considered to have supplied the thermostat because the services they provided were not part of a contract for the erection of a building or a structure. The electrician will not need to comply with any duties in relation to the thermostat.

Likewise, a shipping company that delivers relevant connectable products to distributors on behalf of

the manufacturer is not considered to have supplied those products and will not need to comply with any duties in relation to them.

Clause 56: Meaning of other expressions used in Part 1

232 This clause sets out definitions for

interpreting this Part of the legislation.

Part 2: Telecommunications Infrastructure

Clause 57 : Meaning of "occupier" in relation to land occupied by an operator [J500a]

233 Code rights must normally be granted by the occupier of the land in question. This clause inserts new sub-paragraphs (6A) and (6B) into paragraph 105 of the Code to address situations where the only occupier(s) of land is or are one or more operators who have Code rights in relation to that land, but need to secure new or additional Code rights. In these circumstances, the person who will be able to confer the Code rights sought will be, in effect, whoever would be treated as the occupier of the land were it not for the operator's presence on it.

234 New sub-paragraph (6B)(b) sets out that, if there is no such person, then the operator is able to seek Code rights from every person with an interest in the land whose rights would be prejudiced by the exercise of the Code right

sought.

235 The changes to paragraph 105 of the Code still allow an operator who is exclusively occupying the land to grant Code rights to other operators, who may wish to use the land for the purpose of their networks, as is currently the case.

Clause 58: Rights under the electronic communications code to share apparatus

236 This clause amends various paragraphs of the Code in relation to operators' ability to share the use of their electronic communications apparatus with other operators.

237 Subsection (2) inserts into paragraph 3 of the Code provisions to make the right to share electronic communications apparatus a specific Code right. It also makes corresponding changes to the rights to carry out works on the land and to enter the land so that they reference these activities being carried out for the purpose of sharing such

apparatus. If such a right is agreed or imposed, the Code agreement may include any such terms as are needed to enable the right to be exercised. The provisions make clear that the right to share is a right available solely to an operator who is keeping apparatus on land in accordance with a Code agreement (the "first operator"). The right, where agreed or imposed, provides the first operator with permission to share that apparatus with others. Other operators therefore cannot use paragraph 3 to require the first operator to share that apparatus. As with the other Code rights, a Code right to share apparatus will only be exercisable in accordance with the accompanying terms (see paragraph 12(1) of the Code). See also subsection (4) which deals with terms relating to sharing.

238 The statutory purposes at paragraph 4 of the Code have been amended at subsection (3) to reflect the new right to share in paragraph 3 of the Code.

239 Subsection (4) amends paragraph 9 of the

Code so as to make clear that an agreement under part 2 of the Code can potentially include terms - subject to whatever is agreed by the parties or imposed by a court - permitting the operator on which Code rights are conferred (the first operator) to share the exercise of such Code rights with another operator, in connection with the sharing of the main operator's electronic communications apparatus.

240 Subsection (5) confirms that the new Code rights inserted into paragraph 3 do not automatically apply to existing agreements under part 2 of the Code, and also do not affect any rights already granted in an agreement under part 2 of the Code.

> Example: Sharing apparatus between operators
>
> Operator 1 has a Code agreement with a site provider permitting them to install apparatus on the site provider's land.
>
> Operator 1 is aware that once their apparatus has been installed, other operators may wish to share the use of it.

Under the new paragraph 3, they ask for a right to share their apparatus with others. The site provider agrees that they may have this right, subject to the payment of additional consideration if the sharing involved goes beyond the degree of activity permitted by the paragraph 17 automatic rights to share.

Operator 1 subsequently enters into a commercial agreement with Operator 2, permitting Operator 2 to share use of the installed apparatus. This enables Operator 2 to expand their network without having to carry out non essential build / installation works. In most cases, Operator 2 will need to access the relevant land in order to install their own equipment on Operator 1's apparatus.

Operator 1 must have authority to permit this access, under the terms of their Code agreement with the site provider, or as a result of their own occupation of the land.

Clause 59: Upgrading and sharing of apparatus: subsisting agreements

241 This clause amends Schedule 2 of the Digital Economy Act 2017 (the Electronic Communications Code: Transitional Provision)

to allow operators who have Code agreements pre-dating 28 December 2017 to upgrade and share apparatus under limited circumstances. It does this in subsection (3) by removing the exclusion in paragraph 5 of Schedule 2 to the Digital Economy Act 2017 of the upgrading and sharing rights set out in paragraph 17 of the Code. However, subsisting agreements (defined in paragraph 1 of Schedule 2 to the Digital Economy Act 2017 as an agreement for the purposes of paragraphs 2 or 3, or an order under paragraph 5, of the Telecommunications Act 1984, which was in force and continuing when the Code came into force) remain exempt from the automatic rights to upgrade and share as set out in paragraph 17 of the Code.

242 Instead, subsisting agreements will be subject to the more restrictive rights to upgrade and share apparatus set out in the new paragraph 5A inserted into Schedule 2 to the Digital Economy Act 2017 by subsection (4), which provides for a modified version of the

existing paragraph 17 of the Code ("the modified paragraph 17") to apply in these circumstances. The narrower conditions in the modified paragraph 17 mean that the rights are limited to apparatus installed under land, and are only exercisable where (a) the upgrading and sharing activity will have no adverse impact on the land under which the apparatus is situated; and (b) the upgrading and sharing activity will impose no burden on the other party to the agreement, which includes anything that has an adverse effect on the person's enjoyment of the land or causes them any loss, damage or expense.

243 The exercise of this right is also subject to a notice requirement in the modified paragraph 17, which requires the operator to affix a notice, no later than 21 days before the upgrading and sharing is carried out, in a secure and durable manner, on a conspicuous object on the relevant land. The modified paragraph 17(12) sets out that relevant land is either the land on which the apparatus is

situated, where the operator has a right to enter the land, or in all other cases, the land where the works will be carried out to enable the upgrading and/or sharing of the apparatus to take place.

244 The modified paragraph 17(7) sets out the manner in which the notice must be attached. The modified paragraph 17(8) confirms that any address provided by an operator within a modified paragraph 17(7) notice will be treated as the proper address for any subsequent notices or other documents in accordance with paragraph 91(2) of the Code.

245 The modified paragraph 17(9) makes clear that any terms in a subsisting agreement that prevent, limit or in any other way impose conditions on the rights to upgrade and share electronic communications apparatus where the conditions in the modified paragraph 17(3) and (4) have been met will be void. The modified paragraph 17(10) confirms that the upgrading and sharing rights conferred by the modified paragraph 17 do not confer a right of

entry on to the land. This means that unless an operator already has a right of entry onto the land, it cannot use the rights contained in the modified paragraph 17 to undertake upgrading or sharing which requires entry onto private land.

246 The modified paragraph 17(11) confirms that, as is the case for the current upgrading and sharing rights under paragraph 17 of the Code, references to sharing electronic communications apparatus include carrying out works to the apparatus to enable such sharing.

Clause 60: Upgrading and sharing of apparatus installed before December 2003

247 Subsection (3) inserts a new paragraph 17A into the Code so that when an operator has apparatus under land (such as ducts and cables) that was installed before 29 December 2003 (the date on which the Code came into force), the operator will have a right to upgrade and share that apparatus subject to

the same conditions as those contained in clause 59 above.

248 Subsection (4) amends paragraph 24 of the Code, which is the provision which sets out how consideration is to be determined for an agreement imposed by an order under paragraph 20 of the Code. The amendment to the assumptions in paragraph 24(3) of the Code means that the new automatic right to share, in the new paragraph 17A of the Code as inserted by Clause 60, is not to be taken into account in any way for the purposes of assessing the market value of a person's agreement to confer or be bound by Code rights. This mirrors the provision in paragraph 24 of the Code which disregards the rights in paragraph 17 of the Code, and confirms that the valuation model remains the same notwithstanding the coming into force of the new paragraph 17A right.

Clause 61: Rent under tenancies conferring code rights: England and Wales

249 This clause applies to Code agreements in England and Wales, entered into before 28 December 2017, which are currently subject to Part 2 of the Landlord and Tenant Act 1954 ("the 1954 Act"), and are consequently excluded from the renewal procedures contained in Part 5 of the Code by paragraph 6(2) of Schedule 2 of the 2017 Act. The 1954 Act only applies in England and Wales, and the following amendments therefore have no effect in relation to Scotland or Northern Ireland. The position in respect of Northern Ireland, which also has legislation excluding agreements from the operation of Part 5, is set out at paragraphs 252 to 254 below. There are no equivalent provisions in Scotland requiring amendment for these purposes.

250 If an agreement is renewed using Part 5 of the Code, paragraph 34(11) provides that the valuation framework contained in paragraph 24 will apply in cases where a renewal agreement is imposed by a court order.. This clause inserts a new section 34A into the 1954

Act so that where an agreement is renewed and the primary purpose of that agreement is to grant Code rights, any financial terms of the renewal agreement will be determined by reference to provisions that mirror paragraph 24 of the Code. For completeness, separate provision dealing with the award of compensation is made by clause 63, as discussed below.

251 Subsections (3) and (4) of clause 61 amend sections 24C and 24D (respectively) of the 1954 Act so as to provide that subsections (2) to (4) of the new section 34A will also apply in cases where a court is asked under section 24C or 24D of the 1954 Act to determine whether an interim rent should be paid and how much this rent should be during the renewal process.

Clause 62: Rent under tenancies conferring code rights: Northern Ireland

252 This clause amends Article 18 of the Business Tenancies (Northern Ireland) Order

1996 (‘the 1996 Order”). This clause applies to Code agreements in Northern Ireland, entered into before 28 December 2017, which are protected by the 1996 Order, and are consequently unable to use the Code’s Part 5 renewal procedure.

253 Currently, where an operator is able to renew pursuant to Part 5 of the Code, the amount of rent payable to the site provider will be calculated in accordance with paragraph 24 of the Code. In addition the site provider will be entitled to seek compensation, covering loss and damage pursuant to paragraph 25.

254 So as to provide an approach which is more consistent with that found in the Code, this clause also inserts new Article 18A into the 1996 Order so that, where a subsisting agreement is renewed pursuant to the 1996 Order and the primary purpose of that agreement is to grant Code rights, the rent will be calculated in a way which mirrors the provisions in paragraph 24 of the Code.

Clause 63: Compensation relating to code rights: England and Wales

255 This clause amends the 1954 Act by inserting section 34B, which is designed to mirror the compensation provisions in paragraph 25 of the Code and ensure that site providers have the same rights to compensation where a Code agreement is renewed under the 1954 Act, as they would if it was renewed under the Code. Under this provision site providers will be able to recover amounts for loss and damage which they have sustained or will sustain as a result of the operator exercising any Code rights conferred by the new tenancy..

256 Clause 63 also inserts a new section 34C into the 1954 Act, which sets out the types of loss and damage that can be awarded to the site provider by the court and how those sums will be calculated. It also limits the amount which the site provider can recover, so that the amount cannot exceed the site provider's losses.

Clause 64: Compensation relating to code rights: Northern Ireland

257 This clause amends the 1996 Order by inserting Article 18B, which is designed to mirror the compensation provisions in paragraph 25 of the Code and ensure that site providers have the same rights to compensation where a Code agreement is renewed under the 1996 order, as they would if it was renewed under the Code. Under this provision site providers will be able to recover amounts for loss and damage which they have sustained or will sustain as a result of the operator exercising their Code rights.

258 The provision also inserts a new article 18C into the 1996 Order, which sets out the types of loss and damage that can be awarded to the site provider by the court and how those sums will be calculated. It also limits the amount which the site provider can recover, so that the amount cannot exceed the site provider's losses.

Clause 65: Jurisdiction of court in relation to tenancies in England and Wales

259 This clause inserts a new subsection (2A) into section 63 of the 1954 Act. This provision gives the Secretary of State power to make regulations which enable cases heard under Part 2 of the 1954 Act, where the primary purpose of the current Code agreement is to grant Code rights, to be heard in either the First-tier Tribunal or the Upper Tribunal. This will enable the Secretary of State to provide that all disputes relating to code rights fall within the jurisdiction of the same courts. A change to this effect is not required in relation to the 1996 Order, since disputes under that Order are already dealt with by the Lands Tribunal in Northern Ireland.

Clause 66: Unresponsive Occupiers

260 This clause inserts Part 4ZA into the Code. Part 4ZA makes provision for the courts to confer time-limited rights on an operator who has made repeated requests for Code rights for the purpose of providing an electronic

communications service, and the occupier of that land (as defined in paragraph 105 of the Code) has failed to respond.

Paragraph 27ZA: Introductory

261 This paragraph explains that Part 4ZA makes provision for the court to impose an agreement which allows operators to exercise Code rights in specific conditions. These rights are for the purpose of providing an electronic communications service (defined in section 32 of the 2003 Act) to relevant premises where the occupier or another person with an interest in the relevant land has not responded to repeated notices seeking agreement to confer or otherwise be bound by the Code rights sought.

Paragraph 27ZB: Circumstances in which an application for an order under this Part can be made

262 Sub-paragraph (1) paragraph sets out the circumstances in which an application for an order under Part 4ZA can be made.

Specifically:

a. the operator must intend to provide an electronic communications service to relevant premises;

b. in order to provide that service, the operator must need to install electronic communications apparatus *under* or *over* - but not *on* - the relevant land;

c. in order to install and operate that apparatus, the operator must require a person (referred to in this Part as "the required grantor") to agree to either confer on the operator a Code right in respect of "relevant land" or be bound by such a Code right exercisable by the operator;

d. the operator must have given the required grantor a notice (in accordance with paragraph 20(2) of the Code, which sets out what a request notice must contain) seeking that agreement (referred to as a "request notice"); and

e. the required grantor must have not

responded to the operator.

263 Sub-paragraph (2) sets out the circumstances when paragraphs 27ZC and 27ZD (which provide for requirements to be met before part 4ZA order can be made) do not apply: (a) where the relevant premises falls within the scope of Part 4A and (b) where the relevant land is a ‘connected land’ as defined under paragraph 27B(3) of the Code. This serves to make clear which process - Part 4A or Part 4ZA - should be used, depending on the land which an operator is seeking to access.

264 “Relevant land” is defined in sub-paragraph (3)(a) as meaning land which is any land other than land covered by buildings or used as a garden, park or other recreational area.

265 Sub-paragraph (3)(b) provides for the making of regulations by the Secretary of State to modify the definition of “relevant land”, expanding it so as to include specified types of

land that is covered by buildings or used as a garden, park or other recreational area.

266 Sub-paragraph (4) provides that, before making regulations modifying the definition of relevant land, the Secretary of State must consult various parties, including operators, persons appearing to the Secretary of State to represent owners of interests in land who are likely to be affected by the regulations, and any other person the Secretary of State thinks appropriate.

267 Sub-paragraph (5) makes provision for what constitutes a response by the required grantor. Any engagement in writing - including agreement to the request notice, refusal of it, or any other response to the request notice - by the required grantor with the operator constitutes a response for these purposes.

Paragraphs 27ZC and 27ZD: Requirements to be met before applying for an order under this Part

268 Paragraph 27ZC makes provision about the requirements which an operator has to meet before applying to the court for an order under the new Part 4ZA.

269 Sub-paragraph (1) provides that an operator may not apply for a Part 4ZA order unless it has given the required grantor: (a) two warning notices, and (b) a final notice. These notices are in addition to the initial 'request notice' required by 27ZB(1)(d).

270 Sub-paragraph (2) sets out that a warning notice must be in writing and what that notice must contain.

271 Sub-paragraph (3) provides that the first warning notice may only be given after the end of the period of 14 days beginning with the day on which the 'request notice' was given.

272 Sub-paragraph (4) provides that the

second warning notice may only be given after the end of the period of 14 days beginning with the day on which the first one was given.

273 Sub-paragraph (5) sets out that a final notice must be in writing and what that notice must contain.

274 Sub-paragraph 6 provides that a final notice may only be given within the “permitted period”. This period is defined in sub-paragraph (7) as beginning (a) immediately after the end of the period of 14 days beginning with the day on which the second warning notice was given, and (b) ends at the end of the period of 28 days, beginning with the day on which the second warning notice was given. Taken together, this provides a 14 day window in which a final notice may be given.

275 Sub-paragraph (8) provides power for the Secretary of State to specify by regulations any further conditions that an operator will need to satisfy before issuing a final notice.

276 Sub-paragraph (9) provides that where the word ‘specified’ is used in this paragraph, the item in question may be specified in regulations by the Secretary of State. Items in this paragraph which are ‘specified’ are 1) additional information which must be included in a “warning notice”, 2) additional information which must be included in a “final notice”, and 3) the time period within which the required grantor must respond to the final notice.

277 In paragraph 27ZD, sub-paragraph (1) sets out when an operator is able to apply to the court for a Part 4ZA order. This includes requirements that there has been no previous Part 4ZA order imposing an agreement between the operator and the required grantor in respect of the code rights sought in the request notice, that the operator has met all the requirements related to provision of notice to the required grantor, including giving sufficient time for the required grantor to respond, , the required grantor has not responded to the operator and the operator

has met the specified conditions (see sub-paragraph (6))

278 Sub-paragraph (2) provides that an application for a Part 4ZA order must be accompanied by the evidence specified in any regulations made by the Secretary of State.

279 Sub-paragraph (3) provides that an application may not be made after the end of the specified period (which will be set out in regulations made by the Secretary of State).

280 Sub-paragraph (4) provides that the operator must give notice to the required grantor that it has applied for a Part 4ZA order.

281 Sub-paragraph (5) makes provision for what constitutes a response by the required grantor. Any engagement in writing by the required grantor with the operator constitutes a response for these purposes.

282 Sub-paragraph (6) provides that where the word ‘specified’ is used in this paragraph, the item in question may be specified in regulations by the Secretary of State. Items in

this paragraph which are ‘specified’ are 1) additional conditions which an operator must satisfy before applying to the court for a Part 4ZA order 2) evidence which must accompany an application, as described in sub-paragraph (2), and 3) the time after which an application may no longer be made, as described in sub-paragraph (3).

Paragraph 27ZE: When a Part 4A order can be made and its effect

283 Sub-paragraph (1) provides that the court may make a “Part 4ZA order” if (and only if) (a) the requirements for applying for the order have been met and (b) the required grantor has not objected to the making of the order.

284 Sub-paragraph (2) provides that a Part 4ZA order is an order which imposes an agreement between the required grantor and the network operator by which the required grantor confers specific code rights identified in the request notice in respect of the relevant land, or which provides for the code right

identified in that notice in respect of the relevant land, to bind the required grantor.

285 Sub-paragraph (4) provides that the terms of an agreement imposed by a Part 4ZA order are restricted to those specified in regulations. Those regulations will be made by the Secretary of State subject to the affirmative resolution procedure.

286 Sub-paragraph (5) sets out the terms of the agreement which must be set out in regulations made by the Secretary of State. These include: restricting the operators right to enter land to agreed times except in cases of emergency, imposing requirements on operator's insurance cover and indemnification of the landowner, imposing requirements to restore the land when any works are completed and prohibiting the installation of apparatus on land when the intent is to later install apparatus over or under it.

287 Before making regulations, as set out in sub-paragraph (6), the Secretary of State must

consult interested parties, including those who the Secretary of State believes are likely to be affected by the regulations.

Paragraph 27ZF: Expiry of Part 4ZA code rights

288 Sub-paragraph (1) provides for the circumstances in which a Part 4ZA code right (defined under paragraph 27ZE(3) as code right which is conferred by or otherwise binds the required grantor pursuant to an agreement imposed by a Part 4ZA order) ceases to be conferred on the network operator. Instances where a Code right will no longer apply are a) where a replacement agreement (as defined under sub-paragraph (2)) comes into effect, b) where the court refuses an application by the operator for imposition of a replacement agreement,or c) where the right has not ceased to have effect due to a) or b), at the end of period specified in the agreement as the period during which the code right would have effect (see sub-paragraph (3)).

289 Sub-paragraph (3) provides that "the specified period" is the period of no more than six years, with the actual period to be specified by the Secretary of State in regulations. Those regulations are subject to the negative resolution procedure. The effect of sub-paragraph (3) is that Part 4ZA Code rights will (unless brought to an end sooner, due to the circumstances described in 27ZF(1)(a) and (b) above) cease to have effect at the end of a period lasting no more than six years.

290 Sub-paragraph (4) provides that the required grantor has a right to require the operator to remove the apparatus (subject to Part 6 of the Code) placed under or over the relevant land, when the Part 4ZA order has ceased to have effect or otherwise to bind the required grantor.

Paragraph 27ZG: Compensation

291 Sub-paragraph (1) sets out that this paragraph applies after a court has made a Part 4ZA order

292 Sub-paragraph (2) provides that, if an application for them to do so is made by the required grantor, the court may order an operator to pay compensation to the required grantor for any loss or damage sustained, or that will be sustained by the latter, as a result of the exercise by the former of a Part 4ZA Code right.

293 Sub-paragraph (3) provides that a court may make an order to pay compensation at any time after the Part 4ZA order has been made, including at a time after the Part 4ZA ceases to apply.

294 Sub-paragraph (4) provides that an order made under this paragraph can either a) specify the amount of compensation that the operator should pay, or b) give instructions for how an amount of compensation should be determined.

295 Sub-paragraph (5) provides that if the approach described above at (4)(b) is taken, these instructions may provide for the amount

of compensation to be agreed between the operator and required grantor, or for a dispute about the amount of compensation to be settled through arbitration.

296 Sub-paragraph (6) provides that a compensation order may require the operator to pay compensation in several ways , including making a lump sum payment,periodical payments, on the occurrence of a particular event, or in another form the court seems fit to direct.

297 Sub-paragraph (7) provides that paragraph 84 of the Code (compensation where agreement is imposed or apparatus removed) makes further provision about compensation where a Part 4ZA order has been made.

Paragraph 27ZH: Interpretation of this Part

298 This paragraph sets out the interpretation of various key terms in Part 4ZA of the Code, including “request notice”, “premises” and “required grantor”.

Clause 67: Arrangements pending determination of certain applications under code

299 This clause amends paragraph 35 of the Code so that in cases where one of the parties has applied for an order asking for an expired agreement to be modified or terminated, either party may apply to the court for an interim order, pending determination of the full application.

300 Such an application may seek interim changes to any of the terms of the agreement, including the financial terms. This is in contrast to the present position, which only permits interim applications in relation to expired agreements (i) in relation to the consideration to be paid pending a full determination; and (ii) to be made by a site provider..

301 The clause inserts a new sub-paragraph (4) into paragraph 35, which sets out the factors that the court will need to consider when making the order. These include the operator's business and technical needs and

the site provider's use of the land.

Clause 68: Use of alternative dispute resolution

302 Where an operator requires an occupier of land to give it rights under the Code, it can serve a paragraph 20 notice pursuant to paragraph 20 of the Code setting out the code rights and other terms it is seeking and asking the occupier to agree to those terms.

303 Subsection (2)(a)inserts a new sub-paragraph (2A) into paragraph 20 of the Code, which sets out the process by which an operator must request code rights from an occupier. Under the new provision, operators will be required to provide information about Alternative Dispute Resolution (ADR) with a paragraph 20 notice. ADR may then be an option if the parties are unable to reach an agreement. By placing information regarding ADR in the paragraph 20 notice, it informs the occupier that disputes can be dealt with without the need to proceed to court. This information will then allow the occupier to know that if parties are unable to agree, they may be able to go down the route of ADR to settle the matter.

304 New sub-paragraph (2A)(b) also requires the operator to inform the occupier of the potential consequences of refusing to engage in ADR, namely that the courts can take into account a party's unreasonable refusal to engage in ADR when deciding on what costs order to make at the end of the proceedings.

305 Subsection (2)(b) inserts new sub-paragraphs (5) and (6) into paragraph 20 of the Code so that, where the parties are unable to reach an agreement, there is an additional obligation on an operator to, if reasonably practicable, consider the use of one or more forms of ADR before it makes an application to the courts. If the operator fails to comply with this provision and an application is made to the courts, the courts can consider that failure when deciding on the appropriate costs order. At any time, if the operator decides that it would like to engage in ADR with the occupier , it can notify the occupier in writing.

306 Subsections (3) and (4) insert similar ADR provisions into Part 5 of the Code. Under

paragraph 32 of the Code, as amended by subsection (3), an operator will be required to inform a site provider of the availability of ADR and potential costs consequences of not engaging, when serving a counter-notice. Again, the operator is required to consider ADR, if it is reasonably practicable to do so, before issuing court proceedings. Under this procedure, if at any time either the operator or the site provider decides that it would like to engage in ADR then it can notify the other party in writing. Under paragraph 33 of the Code as amended by subsection (4), the operator will be required to include in its notice details of the availability of ADR, and potential costs consequences of not engaging in that process. This procedure differs from that in subsection (3) as here either party (not just the operator) must consider, where reasonably practicable to do so, whether the use of ADR would be appropriate. If at any time, the operator or the site provider decides that it would like to engage in ADR , it can notify the

other party in writing.

307 Subsection (5) amends paragraph 96 of the Code to place a duty on the court to consider any unreasonable refusal by either party to engage in ADR when making an order as to costs or, in Scotland, expenses.

Clause 69: Complaints relating to the conduct of operators

308 This clause places an obligation on OFCOM to include guidance concerning how operators handle complaints about their conduct in a code of practice published under paragraph 103 of the Code.

Clause 70: Power to impose time limits on the determination of code proceedings

309 This clause inserts a new section 119A into the 2003 Act. This amendment provides the Secretary of State with a power to specify in regulations a time period within which specified proceedings on applications made under the Code must be determined. Such a specification may include the extension or

removal of any time limits, or the application of different time limits to different types of proceedings, provided such proceedings are of the type described in the new section 119A(2). The new section 119A(3) makes clear that in exercising this power, the Secretary of State is able to amend or revoke existing provision made by the Electronic Communications and Wireless Telegraphy Regulations 2011.

Clause 71: Rights of network providers in relation to infrastructure

310 This clause amends the 2003 Act, by inserting a new section 148A into the 2003 Act.

311 Subsection (1) of the new section 148A confers power on the Secretary of State to make regulations concerning the rights of network providers in respect of relevant infrastructure required for the purpose of facilitating the development of public electronic communications networks.

312 Subsection (2) of the new section 148A, read with subsections (3) and (4), provides that

such regulations may make provisions for the following , among other things:

a. require a person to grant the network provider access to relevant infrastructure;
b. require a person to provide the network provider information concerning the relevant infrastructure for specific purposes, provided specific conditions are met.
c. works being carried out of a specified description on such infrastructure;
d. requests by network operators for rights conferred by the regulations, including the procedure for making a request, the form in which the request is to be made, the grounds on which a request can be refused, a duty on a minister to give an opinion if such a request is refused and provision on what effect such an opinion will have, including whether it can be binding on specific persons in specific circumstances (see subsection (3));
e. how information provided pursuant to the

regulations is to be treated;

f. disputes arising under the regulations, including the procedure for dealing with those disputes, the appointment of a person to determine such disputes and the powers which they will have, the time limits for determining such a dispute and how appeals of such decisions will be dealt with (see subsection (4));

g. requiring a specified person to give guidance on the regulations and how such guidance should be published, whether particular persons should be consulted before guidance is given and how often the guidance and the regulations should be reviewed.

313 Subsection (5) of the new section 148 makes provision in respect of Crown interests in land, whilst subsection (6) provides that, in particular, any regulations made under subsection (1) may amend, vary or revoke any provision made by the Communications (Access to Infrastructure) Regulations 2016.

314 Subsection (7) of the new section 148A provides that, before making regulations under subsection (1), the Secretary of State must consult Ofcom and such other persons the Secretary of State considers appropriate.

315 Subsection (8) of the new section 148A provides that regulations made under subsection (1) are subject to the affirmative resolution procedure.

316 Subsection (9) of the new section 148A provides definitions of various key terms used in this new section.

Clause 72: Power to make consequential amendments

317 This clause provides the Secretary of State with a power to, by regulations, make amendments to legislation, including primary legislation made before or during the same session of Parliament as this Bill, that are consequential on Part 2 of this Bill. Any regulations that amend or repeal primary legislation, as defined in subsection (3), are

subject to the affirmative procedure. Any other regulations under this section are subject to the negative procedure.

Clause 73: Meaning of "electronic communications code"

318 This clause clarifies that references to "the electronic communications code" in the Bill are to the Code.

Part 3: Final Provisions

Clause 74: Power to make transitional or saving provision

319 This clause provides a power for the Secretary of State, by regulations, to make transitional or saving provisions in connection with the coming into force of any provision of this Bill. A "transitional" provision manages the transition from one regime to another. A "saving" provision saves the operation of an existing piece of legislation or rule of law.

Clause 75: Regulations

320 This clause provides that any regulations the Secretary of State makes under powers in

the Bill are exercisable by statutory instrument. It also sets out that, with an exception in the case of regulations made under clause 77, regulations made under powers in the Bill may make different provision for different purposes, and may contain supplementary, incidental, consequential, transitional or saving provision. The clause also establishes the normal conditions for use of affirmative resolution procedure and negative resolution procedure.

Clause 76: Extent

321 A detailed analysis of the extent of the Bill can be found at Annex A. Otherwise, this clause is self-explanatory.

Clause 77: Commencement

322 The majority of provisions will come into force in accordance with provision contained in regulations made by the Secretary of State. Clause 27 ('Delegation of enforcement functions'), which allows the Secretary of State to delegate their enforcement functions to another person, will come into force on the day

on which the Act is passed, alongside clause 74 ('Power to make transitional or saving provision'), clause 75 ('Regulations'), clause 76 ('Extent') and clause 78 ('Short title'), and any powers to make regulations under or by virtue of this Act.

Clause 78: Short title

323 This clause is self-explanatory.

Schedule: Unresponsive occupiers: consequential amendments

324 The Schedule provides for related amendments to the 2003 Act.

325 Paragraphs 1 to 3 of the Schedule make various amendments to the 2003 Act.

326 Paragraph 2 amends section 402 to provide that regulations under paragraphs 27ZB(3)(b) and 27ZE(4) of the Code are subject to the affirmative resolution procedure.

327 Paragraph 3 makes various amendments to the Code so that it correctly applies and relates to Part 4ZA.

Commencement

328 The provisions of the Bill will come into force as provided for by clause 77 of the Bill. The notes on that clause above provide further details.

329 The government has stated that relevant economic actors, who will be required to ensure that minimum product security requirements are met in relation to consumer connectable products, will be given time to enable a smooth transition to compliance with the provisions in this Bill. When the government makes a commencement order for relevant provisions in Chapter 3 of Part 1 of this Bill (Product Security Enforcement), it intends that the date of commencement will not be sooner than 12 months after regulations are made to specify security requirements under clause 1.

Financial implications of the Bill

330 The financial costs and benefits of the Bill have been set out in accompanying impact

assessments. The following assessments have been made:

a. Part 1: an impact assessment of the product security measures;

b. Part 2: a *de minimis* assessment of the impacts of the telecommunications infrastructure measures.

Parliamentary approval for financial costs or for charges imposed

331 A Money resolution will be needed in respect of the Bill. A money resolution is required where a Bill authorises new charges on the public revenue – broadly speaking, new public expenditure. There is potential government expenditure arising out of the costs of enforcing Part 1 of the Bill, as well as under clauses 34 and 47(5). The House of Commons will be asked to agree that such expenditure is to be paid out of money provided by Parliament.

332 In addition, a 'paying-in' resolution will be needed to support the express requirement

that monetary penalties be paid into the Consolidated Fund under clause 36(9). This will form part of the money resolution.

Compatibility with the European Convention on Human Rights

333 Section 19 of the Human Rights Act 1998 requires the Minister in charge of a Bill in either House of Parliament to make a statement before Second Reading about the compatibility of the provisions of the Bill with the Convention rights (as defined by section 1 of that Act).

334 The Secretary of State for Department of Digital, Culture, Media and Sport, Nadine Dorries MP, has made the following statement:

"In my view the provisions of the Product Security and Telecommunications Infrastructure Bill are compatible with the Convention rights."

335 The Bill engages Article 6 (right to a fair trial), Article 8 (right to respect for private and family life) and Article 1 of the First Protocol (right to peaceful enjoyment of possessions) to the

European Convention of Human Rights ("ECHR") and, in the government's view, is compatible with the rights set out in those Articles. More detail is given in a memorandum to the Joint Committee on Human Rights, which will be published on the Bill's parliamentary webpages.

Related documents

336 The following documents are relevant to the Bill and can be read at the stated locations:

- Proposals for regulating consumer smart product cyber security, July 2020: https://www.gov.uk/government/publications/proposals-for-regulating-consumer-smart-product-cyber-security-call-for-views
- Government response to the call for views on consumer connected product cyber security legislation, April 2021: https://www.gov.uk/government/publications/regulating-consumer-smart-product-cyber-security-government-response
- Consultation on changes to the Electronic Communications Code, January 2021: https://www.gov.uk/government/consultations/consultation-on-changes-to-the-electronic-communications-code

Annex- Territorial extent and application in the United Kingdom

The provisions of the Bill extend and apply to England and Wales, Scotland and Northern Ireland. No

Legislative Consent Motions are required for this Bill. [15]

Provision	England	Wales		Scotland		Northern Ireland	
	Extends to E & W and applies to England?	**Extends to E & W and applies to Wales?**	**Legislative Consent Motion process engaged?**	**Extends and applies to Scotland?**	**Legislative Consent Motion process engaged?**	**Extends and applies to Northern Ireland?**	**Legislative Consent Motion process engaged?**
Part 1: Product Security							
Chapter 1 - Security Requiremen	Yes	Yes	N/A	Yes	N/A	Yes	N/A

[15] References in this Annex to a provision being within the legislative competence of the Scottish Parliament, the National Assembly for Wales or the Northern Ireland Assembly are to the provision being within the legislative competence of the relevant devolved legislature for the purposes of Standing Order No. 83J of the Standing Orders of the House of Commons relating to Public Business.

ts Clauses 1 - 7							
Chapter 2 - Duties of relevant persons etc. Clauses 8 - 25	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Chapter 3 - Enforcement Clauses 26 - 52	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Chapter 4 - Supplementary Clauses 53 - 56	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Part 2: Telecommunications Infrastructure							
Clauses 57 - 60	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Clause 61	Yes	Yes	N/A	No	N/A	No	N/A
Clause 62	No	No	N/A	No	N/A	Yes	N/A
Clause 63	Yes	Yes	N/A	No	N/A	No	N/A
Clause 64	No	No	N/A	No	N/A	Yes	N/A

Clause 65	Yes	Yes	N/A	No	N/A	No	N/A
Clauses 66 - 73	Yes	Yes	N/A	Yes	N/A	Yes	N/A
Part 3: Final Provisions							
Clauses 74 - 78 Schedule - unresponsive occupiers consequential amendments	Yes	Yes	N/A	Yes	N/A	Yes	N/A

PRODUCT SECURITY AND TELECOMMUNICATIONS INFRASTRUCTURE BILL

EXPLANATORY NOTES

These Explanatory Notes relate to the Product Security and Telecommunications Infrastructure Bill as introduced in the House of Commons on 24 November 2021 (Bill 199)

Ordered by the House of Commons to be printed, 24th November 2021.

© Parliamentary copyright 2021

This publication may be reproduced under the terms of the Open Parliament Licence which is published at www.parliament.uk/site-information/copyright

PUBLISHED BY AUTHORITY OF THE HOUSE OF COMMONS