House of Commons Library

By Esme Kirk-Wade

3 November 2021

Telecommunications (Security) Bill 2019-21, 2021-22

Contributing Authors
Noel Dempsey;
Georgina Hutton;
Joanna Dawson

Image Credits
Communications hardware by Tom Blackwell. Licensed under CC BY 2.0 / image cropped.

Feedback
Every effort is made to ensure that the information contained in these publicly available briefings is correct at the time of publication. Readers should be aware however that briefings are not necessarily updated to reflect subsequent changes.

If you have any comments on our briefings please email papers@parliament.uk. Please note that authors are not always able to engage in discussions with members of the public who express opinions about the content of our research, although we will carefully consider and correct any factual errors.

You can read our feedback and complaints policy and our editorial policy at commonslibrary.parliament.uk. If you have general questions about the work of the House of Commons email hcenquiries@parliament.uk.

Contents

Summary

The Telecommunications (Security) Bill 2019-21, 2021-22 ("the Bill") was introduced in the House of Commons on 24 November 2020. It has completed both Commons and Lords stages, and is now due to return to the Commons for consideration of Lords amendments on Monday 8 November 2021.

The Bill follows a cross-government review of UK telecoms supply chains led by the Department for Digital, Culture, Media and Sport from November 2018 and reporting in July 2019. The review focused on the supply chain arrangements for UK telecoms networks (where and from which companies UK telecoms networks source their equipment) and included an assessment of the wider security regulatory framework for telecoms. It concluded that current regulation needed to be "significantly strengthened" to incentivise operators to prioritise security.

The Bill is set against a backdrop of security-related concerns with the involvement of the Chinese technology company Huawei in telecoms infrastructure in the UK and abroad.

As well as the Telecommunications (Security) Bill, the Government introduced the National Security and Investment Bill 2019-21 on 11 November 2020 to address concerns that foreign investment could be used to undermine the UK's national security. This Bill received Royal Assent on 29 April 2021.

The National Security and Investment Act 2021 provides the Government with new powers to scrutinise and intervene in business transactions, such as acquisitions, for national security reasons. For further details, see the Library briefing: National Security and Investment Bill 2019-21.

Aims of the Bill

The Telecommunications (Security) Bill would bring in a new regulatory framework for telecommunications security. This aims to ensure that public telecommunications providers operate secure and resilient networks and services and manage their supply chains appropriately.

The Bill would place stronger duties and responsibilities on telecoms providers, and provide stronger powers for Ofcom, the UK telecoms regulator, to enforce those duties. The Bill includes new powers for the Secretary of State to set telecoms security requirements in regulations and codes of practice.

The Bill would also give new national security powers to the Secretary of State to impose directions on telecoms providers with regard to "high risk vendors". The Government stated that the Bill would "give the UK one of the toughest telecoms security regimes in the world".

Response to the Bill

The Bill has received broad support from across the House. There is general consensus that cyber-attacks on the telecommunications infrastructure pose a significant threat to national security and that legislation is needed to strengthen the security framework. Some members have commented that the Bill should have been introduced sooner.

Key trade associations have issued brief statements of support for the Bill. This has been described as a "guarded welcome". The telecoms company Huawei has reportedly expressed unhappiness with the proposals.

Progress of the Bill

Second Reading of the Bill took place on 30 November 2020. The Committee Stage then ran from 14-26 January 2021. Technical amendments were moved by the Government and agreed. No other amendments were made.

Opposition amendments covered three major themes: national security, supply chain diversification and parliamentary scrutiny. There was suggestion that a number of these amendments would be returned to at a later stage.

A carry-over motion for the Bill was passed, enabling its continued progress into the next parliamentary session. The Bill's remaining stages in the Commons took place on 25 May.

The Bill was sent to the Lords on 26 May and Second Reading took place on 29 June. It was then debated in Grand Committee over two sittings on 13 and 15 July and progressed to Report Stage unamended. Five amendments were agreed at Report Stage, which would bring effect to three substantive changes to the Bill:

- A Government amendment that would apply a negative resolution procedure to the power to issue codes of practice.
- A non-Government amendment that would require the Secretary of State to report on the impact of the Government's diversification strategy and allow for a debate in the Commons on the report.
- A non-Government amendment that would require the Secretary of State to consider whether to issue a designated vendor direction/similar action where a Five Eyes partner (the US, Canada, Australia and New Zealand) has banned a telecoms vendor on security grounds.

The Bill passed Third Reading in the Lords without division. These amendments will be considered in the Commons on 8 November 2021.

The Bill, Explanatory Notes and Delegated Powers Memorandum have been published on the Bill's page on the Parliament website. The Bill's Impact Assessment, as well as summary factsheets, have been published by DCMS.

1 Background

The Telecommunications (Security) Bill 2019-21, 2021-22 ("the Bill") would bring in a new regulatory framework for telecommunications security.

The Bill follows a cross-government review of UK telecommunications supply chains led by the Department for Digital, Culture, Media and Sport (DCMS) from November 2018: the Telecommunications Supply Chain Review. The review focused on the supply chain arrangements for UK telecoms networks (where and from which companies UK telecoms networks source their equipment) and included an assessment of the wider security regulatory framework.

The Review Report was published on 22 July 2019. It highlighted three key concerns with the UK's telecommunications security framework (discussed further in the sections below):

1. Existing industry practices may have achieved good commercial outcomes but did not incentivise effective cyber security risk management.

2. Policy and regulation in enforcing telecoms cyber security needed to be significantly strengthened to address these concerns.

3. The lack of diversity across the telecoms supply chain creates the possibility of national dependence on single suppliers, which poses a range of risks to the security and resilience of UK telecoms networks.[1]

The Review concluded that current regulation needed to be "significantly strengthened" to incentivise operators to prioritise security. The review recommended that a new statutory telecommunications security framework be created. It also recommended new national security powers for the government to control the presence of "high risk vendors" in UK networks.

In its October 2020 report on 5G security, The Defence Committee concluded that the current regulatory situation for network security was "outdated and unsatisfactory" and urged the Government to bring forward the Telecoms (Security) Bill with "no further delay".

The Telecommunications (Security) Bill was introduced in the Commons on 24 November 2020, during the 2019-21 parliamentary session. Following a carry-

[1] DCMS, Telecoms (Security) Bill Factsheet 1: Overview, 24 November 2020

over motion tabled after the Bill's Second Reading, it resumed its progress in the 2021-22 session.

The Government stated that the Bill would "give the UK one of the toughest telecoms security regimes in the world".[2] It would place stronger duties and responsibilities on telecoms providers, and give stronger powers to Ofcom, the UK telecoms regulator, to enforce those duties.

The Bill includes new powers for the Secretary of State to set telecoms security requirements in regulations and codes of practice. The Bill would also give new national security powers to the Secretary of State to impose directions on telecoms providers with regard to "high risk vendors".

1.1 Telecoms networks as critical national infrastructure

Telecommunications (telecoms) networks, such as broadband and mobile networks, are essential to the smooth functioning of everyday life. Telecoms networks are part of the UK's Critical National Infrastructure (CNI) along with 12 other sectors designated by the Government, such as energy and water networks.[3] Any disruption to telecoms networks has the potential to have a major detrimental impact on peoples' lives, essential services, and the wider economy.

The UK is currently undergoing a major digital infrastructure upgrade (see Box 1 below). The Government has ambitions for the majority of the population to be covered by a 5G signal by 2027 and 85% covered by a gigabit-capable broadband connection by 2025.[4]

The potential social and economic benefits of these technologies rely on having confidence in the security underpinning the infrastructure. These high-speed and high-capacity networks will increasingly support an even wider range of applications and services, interacting with other parts of critical national infrastructure and the economy such as transport, energy and financial services networks.

Increased reliance on these networks makes the security of telecoms infrastructure ever more important. Any down time in the network, for whatever reason, could have greater consequences.

[2] DCMS, New telecoms security law to protect UK from cyber threats, 24 November 2020

[3] Cabinet Office, Public Summary of Sector Security and Resilience Plans, December 2017, p5

[4] HM Treasury, National Infrastructure Strategy, 25 November 2020; DCMS, Future Telecoms Infrastructure Review, 23 July 2017

1 Digital infrastructure explainer: full-fibre and 5G

What is gigabit-capable broadband?

Gigabit broadband means any technology that can deliver speeds of at least 1 gigabit per second (1000 megabits per second). 1 gigabit per second allows a high-definition film to be downloaded in under 1 minute. Gigabit broadband usually means full-fibre technology but can also include the latest cable broadband and future 5G mobile networks.

Full-fibre broadband involves fibre optic cables connected directly to each premises. Fibre cables are more reliable than copper wires and allow much faster speeds. Full-fibre connections were available to 14% of UK properties in May 2020, a figure that is steadily growing. For further background information: see the Library briefing on Full-fibre broadband in the UK.

What is 5G?

5G is the next generation of wireless communications technology. It can deliver very fast speeds with very fast response times and can support many devices at one time. 5G will likely be used for wireless technologies beyond mobile networks. Potential applications include in healthcare, smart cities, manufacturing and agriculture. Mobile operators launched the first 5G networks in some UK cities in 2019.

5G is initially being rolled-out on top of existing 3G and 4G infrastructure (called "non-standalone 5G"). This means 5G will inherit much of the previous infrastructure and impacts choice of equipment suppliers (vendors).

In addition to its importance to critical infrastructure, 5G also has some technical characteristics that create new challenges for security and resilience, including:

- 5G is more likely to use commodity ("off-the-shelf") hardware and software-based functions to control network traffic (called "Network Function Virtualisation"). This creates both challenges and opportunities for security.
- "Core" network functions (such as user authentication) that require the highest levels of security protection may move closer in location to the "edge" of the network (base stations).
- 5G is expected to include greater numbers of base stations than previous mobile networks and will connect more user devices. This means there are more potential sites that could introduce vulnerabilities.
- Security of the 5G network relies on sourcing components that can be considered 'end-to-end trustworthy'. There's been heavy focus on Huawei and their equipment in this regard (see Section 2 of this briefing),

> although it's important to recognise that all networks pose risks to some degree and that all vendors and equipment have potential vulnerabilities.[5]
>
> In the 2020 Spending Review the Government allocated £50 million for 2020-2021 as part of a £250 million "commitment to building a secure and resilient 5G network".[6]

1.2 Cyber security threats

The Government has categorised major cyber attacks on the UK as a top-tier threat to national security.[7] This means that such an attack is highly likely and would also have a high impact. The Government's current strategy on cyber security is set out in the National Cyber Security Strategy 2016-2021.

As a designated piece of CNI, telecoms networks face three main types of threat:

- physical attacks, such as an attacker physically cutting cables;
- cyber attacks from state or non-state actors when a computer system is hacked or disrupted; or
- personnel threats when people with legitimate access to systems create opportunities for physical or cyber attacks.[8]

All of these types of attacks are possible and pose risks. For instance, there has been concern that undersea telecoms cables could be cut or disrupted by the submarines of potentially hostile states.[9] Cyber-attacks and vulnerabilities continue to feature in the news, including prominent incidents affecting WhatsApp and British Airways.[10] In 2019, the National Cyber Security Centre (NCSC), the UK's Government funded technical authority on cyber security, defended the UK from 723 cyber incidents.[11]

There are a variety of actors that pose a threat to UK critical infrastructure (eg cyber criminals, states and state-sponsored groups, and terrorists). The

5 Oral evidence to the Defence Committee, The Security of 5G, 30 June 2020, HC 201 (Q223)
6 HM Treasury, Spending Review 2020, 25 November 2020, para 6.86
7 HM Government, National Cyber Security Strategy 2016-2021, 1 November 2016
8 Parliamentary Office of Science and Technology, Security of UK Telecommunications, August 2018, p1
9 Could Russia cut undersea communication cables?, BBC News, 15 December 2017
10 NCSC, NCSC advice following WhatsApp vulnerability, 14 May 2019; BBC News, British Airways faces record £183m fine for data breach, 8 July 2019
11 NCSC, Fourth Annual Review, 3 November 2020

NCSC has said the most significant threat to the UK telecoms sector comes from hostile state actors.[12]

In the last few years, the UK has attributed a range of malicious cyber activity to Russia and China, as well as North Korea and Iranian actors, based on assessments made by the NCSC. For example, in December 2018 the UK, along with its Allies, announced that a group known as APT10 acted on behalf of the Chinese Ministry of State Security to carry out a malicious cyber campaign targeting intellectual property and sensitive commercial data in Europe, Asia and the US.[13] Also in 2018, the NCSC issued a joint technical alert along with US authorities advising of Russian state-sponsored cyber actors targeting UK network infrastructure devices.[14]

Cyber security threats to UK infrastructure are constantly evolving. There is no single method for an attack. Actors may seek to exploit weaknesses in telecoms equipment, network architecture and operational practices. These weaknesses could arise from a range of risks including involuntary or unknown design defects or by illegitimate actions by individuals.

Vulnerabilities in devices can arise in the supply chain through poor quality equipment and technology, or through deliberate placement (e.g. so-called 'backdoor' vulnerabilities). "Man-in-the-middle attacks" involve data and communications passed along telecoms being covertly intercepted, recorded or altered.

Further details on the types of threats telecoms networks face and the key actors can be found in the Governments' UK Telecoms Supply Chain Review. As part of the Telecoms Supply Chain Review (see below), the NCSC conducted an extensive analysis of the security of the UK telecommunications sector.[15]

[12] DCMS, Telecoms Supply Chain Review Report, 22 July 2019

[13] FCO and NCSC, UK and allies reveal global scale of Chinese cyber campaign, 20 December 2018; NCSC, APT10 continuing to target UK organisations, 20 December 2018

[14] NCSC, Russian state-sponsored cyber actors targeting network infrastructure devices, 15 April 2018

[15] NCSC, Summary of NCSC's security analysis for the UK telecoms sector, 28 January 2020

2 National security concerns about foreign involvement in CNI

There have been long standing security concerns about telecoms supply chains which are not limited to 5G.

In 2013 the Intelligence and Security Committee (ISC) published a report on foreign involvement in the Critical National Infrastructure (CNI) and the implications for national security.[16]

In the UK, telecoms CNI are largely in the hands of private enterprises driven by commercial considerations. However, their decisions may have implications for national security. In its 2013 report, the ISC considered that this gives rise to a potential conflict of interest between the commercial imperative and national security, as a result of increasing private ownership of CNI assets combined with the globalisation of the telecoms marketplace.

The Committee examined the relationship between BT and Huawei, which had begun to supply parts of BT's network in 2007. It noted concerns about perceived links between the company and the Chinese state, particularly in light of China's suspected role in state-sponsored cyber attacks. The Committee acknowledged that Huawei had consistently denied these links but considered that, regardless of any specific threat posed by Huawei, the issue of national security concerns about the involvement of foreign companies in the telecoms supply chain needed to be resolved.

The report concluded that the process for considering national security issues in the context of investment in CNI was insufficiently robust. Given the Government's duty to protect the safety and security of its citizens, it considered this to be unacceptable and recommended that the National Security Council should ensure that there are effective procedures and powers in place. In particular, there should be:

- An effective process by which Government is alerted to potential foreign investment in the CNI;
- An established procedure for assessing the risks;
- A process for developing a strategy to manage these risks throughout the lifetime of the contract and beyond;
- Clarity as to what powers Government has or needs to have; and
- Clear lines of responsibility and accountability.[17]

[16] ISC, Foreign involvement in the Critical National Infrastructure, Cm 8629, 2013

[17] Ibid., para 33

The Government accepted the Committee's conclusion that the processes for considering national security issues were insufficient at time of the original agreement between BT and Huawei. However, it pointed to the creation of the National Security Council in 2010 as a forum for assessing the risks and opportunities associated with foreign investment, bringing together the economic and security arms of the Government.[18]

2.1 Increasing concerns relating to 5G

This issue has come to the fore again recently as new commercial supply agreements for 5G equipment are negotiated worldwide. This, together with the Government's Supply Chain Review, has fuelled an ongoing debate about the use of foreign-supplied products in UK 5G networks, in particular with respect to Huawei.

The ISC announced in April 2019 that it would prioritise consideration of Huawei's role in the UK's telecoms infrastructure as part of a wider Inquiry into national security issues relating to China. In particular the Committee intended to consider whether lessons had been learned from its 2013 report.

In July 2019 the Committee published a statement on 5G suppliers. It endorsed the position then taken by the NCSC that having a larger number of suppliers and implementing stringent security measures to guard against any risk they might pose would increase resilience and competition, and result in higher overall security. However, the ISC also acknowledged the geostrategic dimensions to the decision, including concerns on the part of intelligence sharing partners and the UK's desire for a strong economic relationship with China. It concluded that the Government would need to weigh these geostrategic issues against the time and cost inherent in restricting access to the network to certain companies, and security advice about risks.[19]

As well as the Telecommunications (Security) Bill, the Government introduced the National Security and Investment Bill 2019-21 on 11 November 2020 to address concerns that foreign investment could be used to undermine the UK's national security. This Bill received Royal Assent on 29 April 2021.

The National Security and Investment Act 2021 provides the Government with new powers to scrutinise and intervene in business transactions, such as acquisitions, for national security reasons. It follows a Government consultation and the subsequent National Security and Infrastructure Investment Review in 2018. For further details, see the Library briefing: National Security and Investment Bill 2019-21.

[18] HM Government, Foreign involvement in the critical national infrastructure: government response, 18 July 2013

[19] Intelligence and Security Committee of Parliament, Statement on 5G suppliers, 19 July 2019

3 The Government's position on 'High Risk' Vendors

The Telecommunications Supply Chain Review report published in July 2019 – although making recommendations about the UK's telecoms security framework and supplier diversity – did not include a decision on the Government's position regarding restrictions on "high risk vendors" in UK 5G networks.

The Government first annouced its decision to restrict the use of "high risk vendors" in UK telecoms networks in January 2020. High risk vendors include, but are not limited to, Huawei (see Box 2 below).[20] The restrictions announced in January related to UK telecoms networks generally, not just 5G. The Government, on the advice of the National Cyber Security Centre (NCSC), decided that:

- High risk vendors were to be excluded from sensitive "core" parts of 5G and gigabit-capable networks;
- High risk vendors were to be excluded from sensitive and safety/critical locations such as Critical National Infrastructure; and
- High risk vendor access to non-sensitive parts of the network was to be limited to 35%.[21]

In July 2020, the Government changed its position on Huawei following a technical review by the NCSC in response to US sanctions announced in May (see below), instead opting for its phased removal from the UK's 5G network.[22] The Government clarified its new position in a press release, which stated that:

- Buying new Huawei 5G equipment was to be banned after 31 December 2020.
- All Huawei equipment was to be removed from 5G networks by the end of 2027.
- The existing ban on Huawei from the most sensitive 'core' parts of the 5G network remains.[23]

[20] HC Deb 28 January 2020 c709

[21] DCMS, New plans to safeguard country's telecoms network and pave way for fast, reliable and secure connectivity, 28 January 2020

[22] NCSC, Summary of the NCSC analysis of May 2020 US sanction, 14 July 2020

[23] DCMS, Huawei to be removed from UK 5G networks by 2027, 14 July 2020

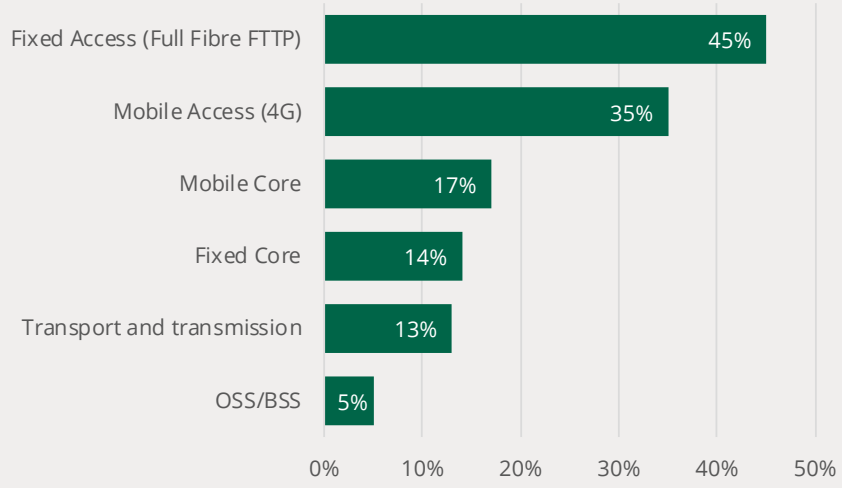
It was also advised that full fibre telecoms providers transition away from purchasing Huawei equipment affected by the US sanctions.

2 How much Huawei equipment is used in UK telecoms networks?

Huawei is a major global supplier of telecoms equipment. It is currently the UK's largest supplier of 4G mobile access equipment, with an overall market share of 35% (see chart below). It is also the largest supplier of full fibre (FTTP) equipment. While Huawei is present in "core" public networks, it is not used in critical Government or military networks.[24]

Huawei's market shares

Measure of market shares vary – Fixed Access (number of homes passed), Mobile and Fixed core (number of subscribers), Transport & Transmission (proportion of traffic), and OSS/BSS (number of subscribers)



Note: Market shares based on data supplied by Huawei to the Supply Chain Review in 2019 and so these may have subsequently changed

Source: DCMS, UK Telecoms Supply Chain Review Report, p. 30

What is a 'high risk' vendor?

The Government describes "high risk vendors" as those that "pose greater security and resilience risks to UK telecoms networks".[25] The NCSC has published advice to telecoms companies that includes a list of non-exhaustive criteria for identifying high risk vendors.[26] Factors include the strategic

[24] Defence Committee, The Security of 5G, 8 October 2020, p42

[25] DCMS, New plans to safeguard country's telecoms network and pave way for fast, reliable and secure connectivity, 28 January 2020

[26] NCSC, NCSC advice on the use of equipment from high risk vendors in UK telecoms networks, 14 July 2020

position and scale of the vendor in the UK and other telecoms markets, the quality and transparency of the vendors engineering, and factors relating to the ownership and operating location of the vendor (such as domestic security laws).

Huawei is considered a high-risk vendor by the NCSC.[27] From a technical perspective, the NCSC has assessed the quality of the company's cyber security and engineering to be low and its processes opaque. From a geostrategic perspective, concerns have been raised that Chinese law could compel Huawei to cooperate with the Chinese intelligence agencies if requested and be ordered to act in a way that is harmful to UK interests (see section 3.2).

A further Chinese company called ZTE has also been deemed high-risk, with the NCSC advising against its inclusion in telecoms infrastructure in 2018.[28]

What sanctions did the US impose on Huawei?

The US first placed Huawei on the Entity List on the 16 May 2019, citing national security concerns.[29] This trade sanction limited the company's access to important US technology for design and production use.

While acknowledging the potential impact this might have on the reliability of Huawei's products, the UK Government, on advice of the NCSC, determined this to be a manageable risk. The restrictions to network access imposed on high risk vendors in January 2020 alongside pre-existing oversight measures (such as the Huawei Cyber Security Oversight Board, see Box 3 below) were considered sufficient mitigation strategies.

On 15 May 2020, the US amended the Foreign-Produced Direct Product Rule (FDPRA) to place further restrictions on Huawei's ability to design or manufacture products using US technology. This means that Huawei must source hardware, particularly computer chips, for its products from other sources.

The UK Government, on advice of the NCSC, viewed this to represent a "significant material change" to the risk posed by Huawei, stating that it could "no longer be confident of being able to guarantee the security of future 5G equipment affected".[30]

---

[27] Ibid.

[28] NCSC, ZTE: NCSC advice to select telecommunications operators with national security concerns, 1 May 2018

[29] U.S. Department of Commerce, Department of Commerce Announces the Addition of Huawei Technologies Co. Ltd. to the Entity List, 15 May 2019

[30] HC Deb 14 July 2020 c1376

3 Huawei Cyber Security Evaluation Centre (HCSEC)

According to the NCSC Huawei and its technology 'has always been considered higher risk by the UK government and a risk mitigation strategy has been in place since they first began to operate in the UK' (see Section 2 of this briefing). [31] The Huawei Cyber Security Evaluation Centre (HCSEC, run and funded by Huawei but jointly overseen and staffed by GCHQ) has since 2010 evaluated the security of Huawei products being used in UK telecoms networks. Although most of the major UK telecoms providers use the HCSEC for information, not all providers do – its use is not mandatory. NCSC technical director Dr Ian Levy stated in February 2019 that, although not perfect, the system had "worked pretty well for the past 8 years". [32]

The Huawei Cyber Security Evaluation Centre (HCSEC) Oversight Board raised concerns in 2018 about Huawei's engineering processes. Its 2019 report confirmed that "no material progress" had been made by Huawei in the remediation of technical issues reported in the 2018 report and highlighted "further significant technical issues" that had not previously been identified. [33]

3.1 Impact of Huawei ban on 5G roll-out

In the Future Telecoms Infrastructure Review the Government stated an ambition to be a world leader in 5G, noting that 5G has the potential to generate "significant economic benefits from the digital transformation of many sectors".[34] The Government set a target that "the majority" of the population would be covered by a 5G signal by 2027.[35]

The Secretary of State for Culture, Media and Sport, Oliver Dowden, acknowledged in July 2020 that additional costs and delays to the roll-out of 5G would result from the Huawei ban:

> We have not taken this decision lightly, and I must be frank about the decision's consequences for every constituency in this country. This will delay our roll-out of 5G. Our decisions in January had already set back that roll-out by a year and cost up to £1 billion. Today's decision to ban the procurement of new Huawei 5G equipment from the end of this year will delay that roll-out by a further year and will add up to £500 million to costs. In addition, requiring operators to remove

[31] NCSC, NCSC advice on the use of equipment from high-risk vendors in UK telecoms networks, 28 January 2020
[32] NCSC, Security, complexity and Huawei: protecting the UK's telecoms networks, 22 February 2019.
[33] HCSEC Oversight board, Annual Report 2019, 28 March 2019
[34] DCMS, Future Telecoms Infrastructure Review, 23 July 2018, p53
[35] Ibid., para 158

> Huawei equipment from their 5G networks by 2027 will add further hundreds of millions of pounds to the cost and will further delay the roll-out. That means a cumulative delay to 5G roll-out of two to three years, and costs of up to £2 billion. That will have real consequences for the connections on which all our constituents rely.
>
> I have to say that to go faster and further beyond the 2027 target would add considerable, and indeed unnecessary, further costs and delays.
>
> The shorter we make the timetable for removal, the greater the risk of actual disruption to mobile telephone networks.[36]

The £2 billion figure is an estimate of the additional costs to operators of removing Huawei equipment from their 5G networks.[37] The Government has said that the exact costs and delays will depend on commercial decisions taken by operators.[38]

Despite calls from some critics for a speedier removal, for example Sir Iain Duncan Smith who argued that some in the industry said it could be completed in five years, the Government has refuted this on practical and economic grounds.[39] Network representatives have suggested that a quicker timescale could result in signal blackouts.[40] Labour Shadow Minister for Digital, Chi Onwurah, argued that the Government had passed the "cost of their mistakes, indecision and poor planning" onto operators and that no further delays should be accepted.[41]

In its October 2020 report on 5G security, The Defence Committee concluded that the 2027 deadline was a "sensible decision" for the time being, although it recommended that:

> Should pressure from allies for a speedier removal continue or should China's threats and global position change so significantly to warrant it, the Government should, however, consider whether a removal by 2025 is feasible and economically viable. The Government should also be alert to the fact that other factors may warrant an earlier removal despite the risk of costs or delays.[42]

In April 2019, prior to the Government's initial decision on high risk vendors, the mobile industry had warned that restrictions on the use of Huawei equipment could cause significant economic and productivity losses.[43] Mobile

---

36 HC Deb 14 July 2020 c1376

37 PQ 74570 [on Telecommunications], 21 July 2020

38 PQ 103501 [Huawei: 5G] 14 October 2020

39 HC Deb 14 July 2020, c1391

40 Oral evidence to the Science and Technology Committee, UK telecommunications infrastructure and the UK's domestic capability, 9 July 2020, HC 450 (Q158)

41 HC Deb 24 November 2020, c374WH

42 Defence Committee, The Security of 5G, 8 October 2020, HC 201, p63

43 Mobile UK, £6.8bn potential risk to UK economy if use of Huawei for 5G rollout is restricted, report finds, 5 April 2019

UK, the trade body for mobile operators, commissioned a report which estimated that a partial or full ban on Huawei in the telecoms supply chain would delay the roll-out of 5G by 18-24 months and cost the UK economy between £4.5 and £6.8 billion. They anticipated that the effects of would be "long lasting and impact not only consumers (through disruption to 4G services and delay in 5G benefit), but whole industries".[44]

Huawei has since commissioned its own report from the same company used by Mobile UK, which revised the estimated economic cost of the ban to £18.2 billion.[45]

Telecoms supply chain diversity

As it currently stands, there are only three potential suppliers of mobile access network equipment in the UK – Nokia, Ericsson and Huawei. The ISC has previously suggested that limiting the field to just two suppliers, on the basis of security concerns about Huawei, could lead to over-dependence on a few suppliers and reduce competition. This in turn could result in less resilience and lower security standards.[46]

The Government published a 5G supply chain diversification strategy shortly after the draft Bill, which aims to address this.

3.2 Geopolitical considerations

As the ISC acknowledged, wider geopolitical considerations have shaped the Government's telecoms security policy. Factors including the UK's intelligence sharing relationships, its desire to have closer economic links with China and the policies adopted by other countries have featured heavily in the debate.

The 'Five Eyes' agreement

The UK has long standing intelligence sharing arrangements with the US, Canada, Australia and New Zealand under the 'Five Eyes' agreement. While the US and Australia took a tough stance on Huawei from the outset, both implementing outright bans, the UK disagreed on the extent to which Huawei posed a security threat. Pressure had been mounting from the US administration in particular for the UK to adopt a policy in line with its own.

Two US lawmakers recently gave evidence to the Commons' Defence Committee, both suggesting that the inclusion of Huawei in the UK's 5G network could threaten the sharing of sensitive intelligence between the US

[44] Assembly, A report for Mobile UK: The Impact on the UK of a Restriction on Huawei in the Telecoms Supply Chain Assembly, 5 April 2019, p3

[45] Assembly, A report for Huawei: Macroeconomic impact of a delayed 5G roll-out in the UK, 9 September 2020

[46] Intelligence and Security Committee, Statement on 5G suppliers, 19 July 2019, p2

and the UK. Senator Tom Cotton expressed the fear that "China is attempting to drive a high-tech wedge between us, using Huawei".[47]

This is not the first time that US officials have threatened the intelligence sharing relationship between the UK and the US on account of its stance towards the Chinese company.[48] However, the Director General of MI5, Andrew Parker, has said that he has no reason to think that the decision would have a negative impact on intelligence sharing with the US.[49]

The UK Government ultimately changed its position on Huawei as a result of US sanctions. The Defence Committee has argued that the Government "should have considered the potential damage to key alliances enough of a risk to begin to remove Huawei from the UK's 5G network before the US sanctions were imposed".[50]

China

Concerns have been raised regarding the nature of the relationship between Huawei and the Chinese state, and the potential risk of espionage or sabotage. Following its recent enquiry on the security of 5G, the Defence Committee concluded that:

> It is clear that Huawei is strongly linked to the Chinese state and the Chinese Communist Party, despite its statements to the contrary. This is evidenced by its ownership model and the subsidies it has received. Additionally, Huawei's apparent willingness to support China's intelligence agencies and the 2017 National Intelligence Law are further cause for concern. Having a company so closely tied to a state and political organisation sometimes at odds with UK interests should be a point of concern and the decision to remove Huawei from our networks is further supported by these links.[51]

The Government had already banned the telecoms equipment supplier ZTE in May 2018, reportedly on the grounds that, with Huawei equipment already in use, it would not be possible to mitigate the risk posed by a second Chinese company.[52]

It has been suggested that the UK was initially reluctant to impose a ban on Huawei due to fears that it might damage economic relations with China, which the Government has sought to strengthen in recent years.[53] Following

47 Defence Committee, The Security of 5G, 8 October 2020, HC 201, p46

48 Trump's repeated threats have 'irritated' the UK and it plans to defy him and strike a deal with Huawei, Adam Bienkov and Thomas Colson, Business Insider, 27 January 2020

49 MI5 head shrugs off risk to intelligence sharing from Huawei links, Financial Times, 12 January 2020

50 Defence Committee, The Security of 5G, 8 October 2020, HC 201, p48

51 Ibid., p51

52 Cyber security watchdog warns UK telcos against using equipment from Chinese supplier ZTE, Financial Times, 16 April 2018

53 Britain Knows It's Selling Out It's National Security to Huawei, Thorsten Benner, Foreign Policy, 31 January 2020

the July decision, China has threatened to withdraw from some areas of the UK's economy, including in critical infrastructure such as nuclear.[54]

Europe

In Europe 5G policy was initially mixed, although in recent months more countries have taken a firmer stance against Huawei.

France has introduced a 'de facto ban' on Huawei 5G equipment by 2028, while it has been reported that Germany is preparing to implement restrictions on telecoms equipment suppliers that will effectively exclude Huawei from 5G. Sweden has imposed an outright ban on the use of Chinese companies Huawei and ZTE in its 5G network.[55]

[54] China threatens to make British companies pay for Huawei ban, The Times, 15 July 2020. For discussion, see the Library briefing paper: New Nuclear (29 July 2020), box 8, p20

[55] Sweden bans Huawei, ZTE from key parts of 5G network, Politico, 20 October 2020

4 Current regulatory framework for telecoms security

The responsibility for the management of security and resilience risks for UK telecoms is currently shared between the Government, Ofcom and industry. Telecoms providers are responsible for assessing risks and taking appropriate measures to ensure the security and resilience of their networks.[56]

The Communications Act 2003, as amended ("the 2003 Act"), is the main regulatory framework for telecoms and applies UK-wide.[57] It sets the main duties and powers of Ofcom – the UK's telecoms regulator.

The 2003 Act requires telecoms providers to take steps to maintain the security and resilience of their networks. The 2003 Act enables Ofcom to audit the measures undertaken by telecoms providers to mitigate security risks. Ofcom has the power to enforce compliance with the requirement to maintain security and may issue penalties for breaches.

Telecoms providers are required to report to Ofcom incidents that "significantly affect the security or availability of the services they provide".[58] Attacks that do not cause service outage do not need to be reported to Ofcom under the 2003 Act.[59] Ofcom is required to publish an annual report summarising the notifications it has received from operators and any action it took in response.[60] These reports are included in Ofcom's annual Connected Nations reports on UK telecommunications infrastructure (see Box 4 below).

There is currently no mandatory security and resilience standard for telecoms networks – this means that neither the Government nor Ofcom can require, by law, that telecoms companies take specific actions regarding security. There are also a number of international standards that telecoms companies can adhere to.

[56] DCMS, Telecoms Supply Chain Review, July 2019

[57] Telecommunications is a reserved matter.

[58] Ofcom, Connected Nations 2019, 20 December 2019 [reissued 18 March 2020], p38

[59] Incidents may need to be reported under other legislation, for example, data breaches must be reported to the Information Commissioner's Office under General Data Protection Regulation (GDPR).

[60] Section 105B of the Communications Act 2003, as amended

4 How often are telecoms incidents reported to Ofcom?

In 2019, Ofcom received 410 reports of significant incidents. Of these, 284 (69%) related to broadband and landline telephones services (fixed services); the remaining 126 related to mobile services.[61] Four incidents were particularly significant, causing disruption to over 1 million customer hours.

Ofcom conducted two investigations into regulatory compliance with the security provisions in the 2003 Act in 2019: the first was into an outage of O2's mobile network that occurred in December 2018.[62] The second was into an outage of BT's (EE's) mobile network that occurred in May 2019.[63] Ofcom did not find breaches of regulatory obligations in either case.

On average, around 35 incidents were reported to Ofcom each month between September 2018 and August 2019.[64] Ofcom stated that in 2019 incidents continued to occur with roughly the same frequency, root causes and level of impact as in recent years. The pattern of where the most incidents occur generally follows population density.

What kinds of incidents are reported?

The main factors causing or contributing to an incident reported to Ofcom include hardware failure, power cuts, and cuts or breaks in cables. Cyber attacks are rarely reported to Ofcom, with none being reported in 2019. Ofcom explained that this could be because the motivations behind cyber attacks are more often associated with, for example, stealing customer data and committing fraud, rather than causing a service outage.[65]

As part of the Telecoms Supply Chain review and its analysis of telecoms security, the NCSC developed Telecoms Security Requirements for the sector.[66] The NCSC explained that the purpose was to set realistic baseline security controls to reduce the risk of security compromises, recognising that no system can be 100% secure:

> Through practical controls, we want to make it hard for an attacker to compromise a UK network, make it likely that any such compromise will be noticed quickly and the harm and impact limited, and make remediation as simple as possible… the TSRs define an achievable baseline of security controls to protect operator networks from realistic and nationally significant cyber attacks. The

[61] Ofcom, Connected Nations 2019: annual report, 20 December 2019 [reissued 18 March 2020]
[62] Ofcom, Investigation into Telefónica UK Limited's compliance with section 105A(4) of the Communications Act 2003, 1 November 2019
[63] Ofcom, Investigation into BT's (including EE's) ("BT") compliance with its regulatory obligations, 5 October 2020
[64] Ofcom, Connected Nations 2019: annual report, 20 December 2019 [reissued 18 March 2020]
[65] Ibid.
[66] NCSC, Summary of NCSC's security analysis for the UK telecoms sector, 28 January 2020

> TSRs are presented within a broader framework that describes the risk that motivates the requirement, and guidance on the implementation and testing of the requirement.[67]

The NCSC intends the framework to be subject to regular and periodic review to ensure it can respond to evolving cyber risks and to reflect advancing best practice.

4.1 Other Ofcom work on security

Ofcom also conducts other programmes of work with the telecoms industry to strengthen the security of the sector that isn't set in legislation.

In 2019, Ofcom launched a Security Resilience Assurance Scheme. This was an "information-gathering exercise to build a more detailed understanding of the security and resilience arrangements" that major communications providers have in place. It provided a "foundation of understanding" to support activities to strengthen telecoms security going forward and understand how companies will be impacted by the legislation contained in this Bill.[68]

Intelligence-led penetration testing: TBEST

Over the last few years DCMS, Ofcom, the NCSC and industry have been developing a programme of threat intelligence-led penetration testing called TBEST.

Penetration testing is the process of running an authorised, controlled test on an organisation to identify vulnerabilities that an attacker could exploit. It uses techniques known to be used by cyber criminals and hostile states. This can include organisational factors such as staff activities, physical access security and can test incidence response plans in action.[69]

Penetration testing services are available commercially and some operators will contract providers to carry out such tests, or use internal resources to conduct testing. TBEST, however, is a regulator-led scheme that draws on Government-provided intelligence that is tailored to the sector and specific organisations involved. It is based on a successful scheme developed by the UK's financial services sector.[70]

---

[67] NCSC, NCSC's security analysis for the UK telecoms sector, 28 January 2020, p17

[68] Ofcom, Our network security and network resilience work, 10 November 2020

[69] Ofcom, Our network security and network resilience work, 10 November 2020

[70] Called CBEST. See Joint Committee on the National Security Strategy Report, Cyber Security of the UK's Critical National Infrastructure, HC1708, 2017-19, para 53-57

TBEST is currently voluntary; providers agree to allow an external testing team to "attack" their network using agreed scenarios. Senior management are aware that the test is being conducted, but most employees are not.

TBEST allows Ofcom, Government and industry to proactively identify specific areas where telecoms security can be improved and to implement appropriate changes. In its security analysis for the Telecoms Supply Chain Review, the NCSC recommended that operators establish a sustained programme of network testing supported by TBEST, stating that network security testing of live telecoms networks is "essential to establishing the true cyber risk to telecoms networks".[71]

[71] NCSC, NCSC's security analysis for the UK telecoms sector, 28 January 2020

5 The Bill

The Telecommunications (Security) Bill ("the Bill") introduces a new security framework for the UK telecoms sector in line with recommendations from the Telecoms Supply Chain Review. The Bill would place stronger duties and responsibilities on providers, and provide stronger powers for Ofcom, the UK telecoms regulator, to enforce these. The Bill also introduces new national security powers that would enable the Secretary of State to impose directions and requirements on network and service providers.

Much of the Bill would add sections to the Communications Act 2003, as amended (the "2003 Act"), which is the current regulatory framework for telecommunications security (see Section 4). The Bill replaces sections 105A to 105D of the 2003 Act with a series of longer and more detailed provisions.

The Bill applies to public telecoms providers. This means operators that provide networks and/or services that are wholly or mainly for use by the public.[72] It includes large companies such as BT, Vodafone and Virgin Media, as well as smaller companies.

Clause numbers in this section refer to those in the Bill 216 2019-21 version of the Bill.

5.1 Duties of telecoms providers

Clauses 1-4 of the Bill would obligate telecoms providers to take measures to mitigate security risk, respond appropriately to security compromises, adhere to codes of practice (for security measures) which may be issued by the Secretary of State, and inform service users and Ofcom of security breaches.

Specifically, **Clause 1** substitutes sections 105A to 105D of the 2003 Act with new sections 105A and 105B. New section 105A would require telecoms providers to take "appropriate and proportionate" measures to identify, mitigate and prepare against the risks of security compromises occurring. A security compromise is defined as "anything that compromises the availability, performance, or functionality of the network or service, or that compromises the confidentiality of the signals conveyed by means of the network service".[73]

Such measures would include service providers carrying out a risk assessment in relation to their network or service, and designing these to minimise the

[72] The term "public communications provider" is defined in Section 151 of the Communications Act 2003.
[73] DCMS, Telecommunications (Security) Bill: Explanatory Notes, 24 November 2020, p10

risk of security compromises, for example, by segregating the most sensitive controls from the rest of the network. Preparing against the risk of security compromises would include measures such as retaining copies of information that would enable the running of functions that are "most critical" to a network or service in the event these were compromised, or having procedures in place to identify security compromises.[74]

Subsections 3 and 4 of section 105A lists exemptions to the definition of a security compromise to enable conduct which is required and authorised by other legislation, for example, the Investigatory Powers Act 2016.

Section 105B, as inserted by the Bill, would enable the Secretary of State to make regulations prescribing specific security measures that telecoms providers must follow. This power would be subject to the **negative procedure.** The Government would "engage with any telecoms providers on the technical detail of secondary legislation before it is finalised, during the passage of the Bill" as well as publish an impact assessment. Any requirements under this provision would be enforced by Ofcom.[75]

The Government has stated that any prescribed security measures would include:

> targeted action to make sure telecoms providers securely design, construct and maintain network equipment that handles sensitive data; reduce supply chain risks; carefully control access to sensitive parts of the network; and make sure the right processes are in place to understand the risks facing their company's public networks and services.[76]

Clause 2 would insert new sections 105C and 105D into the 2003 Act, which would require providers to take measures in response to security compromises, as defined in **clause 1**. Essentially, this means that should a security compromise occur, telecoms service providers would have to "take such measures as are appropriate and proportionate for the purpose of preventing adverse effects (on the network or service or otherwise) arising from the security compromise". Equally, if an adverse effect on a network or service occurred as a result of a security compromise, providers would be required to take measures to remedy or mitigate that effect.

Section 105D would enable the Secretary of State to prescribe security measures to providers in response to security compromises – these powers are subject to the **negative procedure.**

Clause 3 would insert sections 105E to 105I into the 2003 Act, which would enable the Secretary of State to issue codes of practice giving guidance for providers to follow in order to meet their security obligations. An initial code of practice would define three tiers of telecoms providers, and the biggest,

[74] Ibid., p10

[75] DCMS, Factsheet 2: New Telecom Security Framework, 24 November 2020

[76] Ibid.

most important, providers would be subject to the most intensive monitoring and oversight.[77] The clause specifies the procedures that the Secretary of State must follow when issuing, revising, re-issuing or withdrawing codes of practice, including a requirement to consult. Although the Secretary of State would be required to lay codes of practice before Parliament, their issue or withdrawal would require **no parliamentary procedure**.

Sections 105H "makes clear that codes of practice are guidance and that a failure to act in accordance with their provision does not of itself make a provider liable to legal proceedings", although "when determining any question in legal proceedings, the court must take into account any provisions which were in force at the time and appear relevant".[78] Section 105I allows Ofcom to notify a provider where Ofcom determines it is "failing or has failed to act in accordance with a code". The Bill introduces a "duty to explain failure" whereby if providers receive a notification from Ofcom they must give a statement either confirming or denying Ofcom's suspicions along with an explanation.

Clause 4 would insert sections 105J to 105L into the 2003 Act and would require providers to proactively report significant risks to, and breaches of, security to Ofcom, as well as informing the users of the telecoms networks and services of the associated risks. Clause 4 is designed to transpose the intent of the security aspects of the European Electronic Communications Code (an EU directive which regulates telecoms networks and services).

Section 105J would require providers to take reasonable steps to inform users of the existence of the risk, the nature of the security compromise, the steps that users could reasonably undertake in response and the name and contact details of a person for further information. Section 105K would require providers to notify Ofcom as soon as reasonably practicable of any security compromise that would have a significant effect on the network or service. Once notified of a security compromise, Section 105L would require Ofcom to notify the Secretary of State of the risk of compromise (or occurrence) if it could (or already had) have specified serious consequences, such as a threat to national security.[79] Ofcom would be able to notify relevant authorities, service providers or the general public if deemed necessary to help mitigate the risk or effect of a security compromise.

5.2 Role of Ofcom

Clauses 5 to 7 detail the proposed duties and powers Ofcom would have to monitor and, if necessary, enforce its security obligations. The Bill would provide Ofcom with stronger regulatory powers to enforce the new regime. Ofcom's annual budget is approved by its Board and must be within a limit set

[77] Ibid.
[78] Ibid., p13
[79] Ibid., p14

by the government. The Government has said that this will be adjusted to take account of the increased costs of carrying out its enhanced security role.[80] The Bill's Impact Assessment estimated that Ofcom would have increased costs of between £5.4 to £8.9 million over the period 2020-2029 to monitor the compliance of providers.[81]

Further details of Ofcom's new powers and funding arrangements can be found in Factsheet 4: Ofcom and Telecoms Security published by the Department for Digital, Culture, Media and Sport.

Clause 5 would insert a new section 105M into the 2003 Act placing a new general duty on Ofcom to seek to ensure that providers comply with their security duties. Ofcom would be able to issue assessment notices so that it could assess the compliance of providers with security obligations. The assessment notice may place duties on the provider including to undertake specific network testing, allow staff to be interviewed and allow access to premises to inspect equipment and observe tests. Ofcom could require network tests that risk causing a security compromise, if the test consists of techniques that might be expected to be used by a potential attacker –for example, penetration testing (see section 4.1).

Providers would have an obligation to comply with any assessment notice given by Ofcom and bear the cost of any assessment. Ofcom could issue penalties to providers for contravening security duties which include fines (up to 10% of turnover) and suspension or restriction of entitlement to provide services. In cases where there were continued contraventions of security duties, Ofcom could issue further financial penalties ranging from up to £50,000 per day to up to £100,000 per day, with a maximum value of £10 million depending on which provision is breached.

Clause 8 makes provision for civil liability for contravention of security duties by providers. For example, a person who suffers loss or damage as a result of a security breach may bring legal proceedings against the respective provider. It is a defence for a provider to demonstrate that they took all reasonable steps and exercised all due diligence in attempting to avoid security breaches. Ofcom would have to consent to the bringing of proceedings, which may be subject to conditions relating to the conduct of the proceedings.

Clause 10 detail how Ofcom would be obligated to publish a statement of policy explaining how they would ensure compliance with security duties. **Clause 11** would require Ofcom to report annually on security matters to the Secretary of State, and **clause 12** sets out Ofcom's powers to require and share information concerning the security of public electronic communications networks and services.

Clause 24 would insert new section 139ZA, enabling Ofcom to issue higher penalties than those currently set out in the 2003 Act in the case of

[80] DCMS, Factsheet 4: Ofcom and Telecoms Security, 24 November 2020

[81] DCMS, Telecommunications (Security) Bill: Impact Assessment, p45

contravention of requirements to provide information to Ofcom for the purpose of its functions as set out in new sections 105L-105Z, or preparing a report under new section 105Z12 (**clause 18**). The maximum penalty would be set at £10 Million, or £50,000 per day for a continued contravention. Existing penalties are capped at £2 million, or £500 a day.

5.3 Review of the security framework

Clause 14 states how the Secretary of State would be required to review the impact and effectiveness of **clauses 1 to 13** at least every five years. The Secretary of State would have to publish and lay a report before Parliament after each review. The first report would have to be published within five years of the day on which the Act is passed.

5.4 Designated vendor directions

The second part of the Bill **(clauses 15 to 23)** would create new national security powers in the form of "designated vendor directions". While it is not explicitly stated in the Bill, this is intended to address the risk posed by 'high risk' vendors (see section 2.1), conferring on the Secretary of State to power to restrict, prohibit or require the removal of "designated vendors" from the telecoms network. **These clauses would insert new Sections 105Z1 – 105Z28 into the 2003 Act.**

Issuing a direction

The Bill sets out two distinct parts to the process of issuing a designated vendor direction. The Secretary of State would be able to designate a 'high risk' supplier as a "designated vendor" (by issuing a designation notice). This would in turn give the Secretary of State the power to give directions to providers regarding the use of that vendor (a "designated vendor direction").

Clause 15 would give the Secretary of State the power to give a designated vendor direction. This would impose requirements on the use of goods, services or facilities that are supplied, provided or made available by a specified vendor in the telecoms network. This could consist, among other things, of restricting or prohibiting their use or requiring their removal, disabling or modification. The clause would impose a duty on providers to comply with directions.

It would only be possible to use this power in the interest of national security and the requirements of the direction would need to be proportionate to the security risks identified.

A direction would be required to specify which providers it applies to, when it comes into force and the reasons for which it was given, provided this was not

deemed a risk to national security. The specification of a reasonable time period for compliance would be required.

New section 105Z7 would give the Secretary of State the power to require a provider to produce a plan setting out the steps it would take to ensure compliance with the direction.

Clause 16 sets out the Secretary of State's power to designate vendors (through issuing a "designation notice"). The Explanatory Notes summarise factors affecting national security that the Secretary of State may take into account when considering whether to designate a vendor, including:

- the strategic position or scale of the vendor in UK networks;
- the strategic position or scale of the vendor in other telecoms networks, particularly if the vendor is new to the UK market;
- the quality and transparency of the vendor's engineering practices and cyber security controls;
- the vendor's resilience both in technical terms and in relation to the continuity of supply to UK operators;
- security laws in the jurisdiction where the vendor is based and the risk of external direction that conflicts with the interests of national security;
- the relationship between the vendor and the vendor's domestic state apparatus;
- the availability of offensive cyber capability by that domestic state apparatus, or associated actors, that might affect the national security of any country or territory.[82]

The Government has published illustrative drafts of a designated vendor notice and designated vendor direction relating to Huawei specifically.[83] These demonstrate how it intends to exercise the powers contained in the Bill to restrict the use of Huawei equipment and services in UK telecoms networks, in accordance with the ban announced in July 2020 (see section 3).

Prior to giving a designated vendor direction or issuing a designation notice, the Secretary of State would be required to consult the telecoms providers to which the direction applies and the vendor to which it relates, where practical and provided this is not contrary to the interests of national security. They would also be required to periodically review directions and would have the power to vary or revoke them as seen fit.

---

[82] DCMS, Telecommunications (Security) Bill: Explanatory Notes, 24 November 2020, p8

[83] DCMS, Telecommunications (Security) Bill: Illustrative designated vendor direction and designation notice, 30 November 2020

The power to issue a designated vendor direction or notice would **not require parliamentary procedure**, with the exception of the laying of documents before Parliament, as stipulated by **clause 17**.[84] The Secretary of State would not be required to lay copies of vendor directions before Parliament if this was considered likely to prejudice to an unreasonable degree the commercial interests of any person, or contrary to national security interests.

Monitoring compliance

The Bill contains provisions to enable the Secretary of State and Ofcom to monitor the implementation of designated vendor directions.

Clause 18 would give the Secretary of State the power to issue "monitoring directions" to Ofcom, requiring Ofcom to obtain information relating to a provider's compliance with a designated vendor direction and to report this information to the Secretary of State.

Subsections 1 and 2 of new section 105Z13 would give the Secretary of State the power to publish or disclose a report provided by Ofcom under a monitoring direction, keeping in mind the need for confidentiality regarding certain matters.

Subsections 3 and 6 would further amend the 2003 Act to allow Ofcom to require information for use in a report and prevent such decisions from being subject to appeal under the Competition Appeals Tribunal.

Clause 19 would give Ofcom the power to issue inspection notices where it had been given a monitoring direction by the Secretary of State to assess whether a provider is complying with a designated vendor direction. An inspection notice could impose a duty on providers to take a number of actions, as outlined in subsection 4 of new section 105Z14, including to make persons available for interview and to permit Ofcom access to specified premises in order to carry out surveys and collect information. There are limitations on what an inspection notice would be able to require, for example it could not require providers to take actions that would violate legal privilege. Subsection 7 stipulates that an inspection notice must give 28 days notice before requiring any actions from providers.

Inspection notices would be required to set out the consequences for failure to comply and providers would be expected to cover any 'reasonable' costs incurred by Ofcom while gathering information. Noncompliance with a duty imposed by an inspection notice could incur a maximum penalty of £10 million, or £50,000 per day in cases of continued contravention.

Clause 22 would give the Secretary of State the power to request nondisclosure of the content of certain documents and consultations, should their disclosure be determined contrary to interests of national security.

[84] DCMS, Memorandum concerning the Delegated Powers in the Telecommunications (Security) Bill for the Delegated Powers and Regulatory Reform Committee, 24 November 2020, p14

Noncompliance with nondisclosure requirements would hold a maximum penalty of £10 million, or £50,000 per day in cases of continued contravention.

Clause 23 would give the Secretary of State the power to require from any relevant person, in particular those who are or have been providers, information that would support its monitoring efforts and inform decisions regarding designated vendor directions. A notice would need to be issued prior to such a request.

As with other monitoring procedures, the maximum penalty for the contravention of an information request would be £10 million, or £50,000 per day in cases of continued contravention.

Enforcement

The power to enforce a designated vendor direction would sit with the Secretary of State rather than Ofcom. **Clauses 20 and 21** contain provisions for enforcement in response to non-compliance.

Clause 20 sets out processes for the Secretary of State to follow in the event that a provider is considered not to be complying with the requirements of a designated vendor direction. In such a case, the Secretary of State would be able to issue a notification of contravention. As stated in subsection 2 of new section 105Z18, the notification would specify the contravention determined to have taken place and detail steps the provider must take to remedy this. It would also include a deadline for a response from the provider and specify the penalty for non-compliance.

In the case of multiple contraventions, a separate penalty may be specified for each one. In the case of continued contravention, the penalty may relate to any period during which the contravention occurred, and a daily penalty may be applied should contravention continue following receipt of a notification.

Once the deadline for response had expired, the Secretary of State would have to give a decision either confirming the requirements of the notification ("a confirmation decision"), or inform the provider that no further action will be taken. A confirmation decision could require immediate compliance with the requirements of the notification, or specify a time frame for action to be completed within. It would also confirm or amend the sum of the penalty and set a deadline for payment.

A penalty would be required to be 'appropriate and proportionate', with a maximum value of 10% of the providers turnover during the relevant period of contravention or £100,000 per day. This has been described as "a typical threat for telecoms companies for persistent poor behaviour".[85]

[85] UK telecoms groups face huge fines for Huawei breach, Financial Times, 24 November 2020

Should a notification of contravention be issued in the case of a provider failing to provide a plan for compliance with a direction, as required in new section 105Z7 (discussed above), the maximum penalty would be £10 million or £50,000 per day. The Secretary of State may enforce a provider's duty to comply in civil proceedings, as outlined in subsection 9 of section 105Z20.

Clause 21 would give the Secretary of State the power to issue an "urgent enforcement direction" in serious cases of contravention, whereby a significant threat to national security or the network is posed. An urgent enforcement direction would have to specify the contravention that had occurred and the actions that a provider was required to take to remedy this and ensure compliance. It would set out a deadline that this must be completed by. It would not be necessary to specify the reason for the direction should this be considered contrary to national security interests.

The recipient of an urgent enforcement direction would have a duty to comply, which would be enforceable through civil proceedings.

5.5 Maximum penalties

The Bill would give the Secretary of State the power to amend the maximum penalties for contravention of duties and requirements (Henry VIII powers). These powers would be subject to the **draft affirmative procedure**.[86]

5.6 Territorial extent and commencement

The Bill extends and applies to the whole of the United Kingdom. Telecommunications and wireless telegraphy are reserved matters under the devolution settlements. National security is also a reserved or excepted matter.

Clauses 1 to 3 (so far as they confer power to make regulations and issue codes of practice)**, 14, 25 (section 1 and 3), 26 to 29** of the Bill will come into force on the day in which the Act is passed.

Clauses 15 to 24 will come into force at the end of the period of two months from the date the Act is passed.

The remaining clauses will be brought into force by regulations made by the Secretary of State.

[86] DCMS, Memorandum concerning the Delegated Powers in the Telecommunications (Security) Bill for the Delegated Powers and Regulatory Reform Committee, 24 November 2020, p5-6

6 Initial reaction to the Bill

During a debate in the Commons following the Bill's publication, Chi Onwurah, Shadow Minister for DCMS, welcomed the measures taken to improve telecoms security but called for the publication of the Government's diversification strategy:

> The official Opposition welcome the measures taken to secure our network, but without the diversification strategy, our network will not be secure because we will be so dependent on perhaps two vendors. We have to have a diversification strategy, not only to ensure the opportunities in different sectors and different parts of our country in terms of economic development, but to make that network secure. Where is the diversification strategy? How can we have a Bill that does one thing, which is to secure the network, that is so dependent on a strategy that does not appear to be mentioned?[87]

While little commentary had been published at the time of Second Reading, key trade associations did issue brief statements of support for the Bill. This was described as a "guarded welcome". [88] Mobile UK, the trade body for mobile operators, said that it supported the framework of the Bill:

> Network security and resilience have always been a top priority for the UK's mobile network operators. We support the framework for the Telecoms Security Bill and will continue to work closely with the Government to ensure the objectives of the Bill are fulfilled and to build on the already robust security measures mobile operators have in place.[89]

Andrew Glover, Chair of the Internet Service Providers Association (ISPA), reportedly said that ISPA would work with members and policymakers on the Bill:

> Security and resilience have long been priorities for internet service providers as secure and robust networks are at the heart of delivering fast and reliable broadband. The UK currently has high cyber security standards, and this new and updated telecoms security framework will build on this as the threat landscape continues to evolve.

[87] HC Deb 24 November 2020 c374WH

[88] UK telecoms industry gives guarded welcome to Telecommunications Bill proposal, Joe O'Halloran, Computer Weekly, 24 November 2020

[89] Mobile UK, Statement: Telecommunications (Security) Bill, 24 November 2020

> ISPA will be working closely with our members and policymakers on the bill so that it provides a clear and workable set of rules to further protect users, and gives clarity to our members who are upgrading the UK's broadband infrastructure and connecting consumers and businesses throughout the UK.[90]

While voicing general support for the Bill, techUK, a tech industry trade body, also called on the Government to publish its diversification strategy:

> Gigabit connectivity is an essential driver of a levelled up economic recovery. We support the Government's drive to strengthen security and maintain trust in our telecoms networks.
>
> Government has promised an accompanying Diversification Strategy to expand the number of vendors available in the UK. It must deliver on this promise with a strategy that is ambitious, fully funded and maximises opportunities for UK companies in areas such as software, small cells and semiconductors.[91]

The telecoms industry has previously expressed concerns towards the lack of diversity within the supply chain on multiple occasions, with several key industry figures raising the matter while giving evidence as part of the Defence Committee's recent inquiry into the security of 5G.[92] techUK launched a campaign to promote diversification.[93]

Jimmy Jones, Cyber Security Telecoms expert at the cyber security company Positive Technologies, highlighted the higher financial penalties as an effective means of enforcement:

> "The new fines announced today for operators that are not meeting standards are another major financial incentive to get security in order. The security obligations – which include rules on who has access to sensitive parts of the "core" network, how security audits were conducted, and protecting customer data – will force operators to improve their security protection for the whole network rather than just 5G."[94]

Huawei's Vice-President, Victor Zhang, reportedly condemned the Bill as "politically-motivated and not based on a fair evaluation of the risks." He further stated that "it does not serve anyone's best interests as it would move Britain into the digital slow lane and put at risk the Government's levelling up agenda."[95]

---

[90] Internet companies face £100,000-a-day fine if they don't follow Huawei ban, Government reveals, The Telegraph, 24 November 2020

[91] techUK, techUK comments on the Telecommunications Security Bill, 24 November 2020

[92] Defence Committee, The Security of 5G, HC 201, 8 October 2020

[93] techUK, techUK's Diversifying Telecoms campaign, 25 September 2020

[94] UK security law targeting telecoms, Security News Desk, 24 November 2020

[95] UK security bill sets out penalties if telcos use Huawei equipment, Telecoms Tech News, 24 November 2020

7 Summary of Second Reading

The Telecommunications (Security) Bill had its Second Reading on 30 November 2020. It received broad support across the House. There was general consensus that cyber-attacks on the telecommunications infrastructure posed a significant threat to national security and that legislation was needed to strengthen the security framework. Some members commented that the Bill should have been introduced sooner.

The Secretary of State for DCMS (Oliver Dowden) opened the debate, outlining the intentions of the Bill:

> This Bill acts on the recommendations of the United Kingdom telecoms supply chain review, which in turn was informed by the expert technical advice at the National Cyber Security Centre in GCHQ. First, it establishes a tough new security framework for all the UK's public telecoms providers. This will be overseen by Ofcom and the Government, and they will have a legal duty to design and manage their networks securely. Rigorous new security requirements will be set out in secondary legislation, and codes of practice will set technical guidance on how providers should meet the law, and where providers are found wanting, Ofcom will have the power to impose steep fines.
>
> [...]
>
> If we pass this Bill, few other countries in the world will have a tougher enforcement regime, and the point of this Bill is not just to tackle one high-risk vendor; it raises the security bar across the board and protects us against a whole range of threats. According to the NCSC, the past two years have seen malicious cyber-activity from Russia and China as well as North Korea and Iranian actors. While I know that telecoms providers are working hard to protect our networks against this hostile activity, the Government have lacked the power to ensure they do so. This Bill puts a robust security framework in place, guaranteeing the protection of our networks.[96]

The Secretary of State detailed how the Bill would be used to monitor and enforce the decision to remove Huawei from the 5G network by 2027 (see section 3). He acknowledged concerns that the Bill does not explicitly name Huawei, defending this decision on the grounds that:

> First, as we discussed, this Bill is designed to tackle not only the Huaweis of today but the Huaweis of tomorrow, wherever they come

[96] HC Deb 30 November 2020 c70

> from. It needs to be flexible enough to cover future threats and not tie our hands by limiting our response to one company and one company alone. Secondly—this is the most crucial point—making reference to any one company would create a hybrid Bill, dramatically slowing the passage of the Bill and therefore our ability to combat all high-risk vendors, including Huawei.[97]

The Labour Shadow Secretary of State for DCMS (Jo Stevens) raised the following concerns, which were echoed by members on both sides of the Chamber:

- The handing of "huge" national security powers to the Secretary of State, highlighting the lack of a definition of 'national security' and concerns towards limited opportunity for parliamentary scrutiny.
- Whether Ofcom's resources and expertise are sufficient to fulfil its new statutory duties.
- The effectiveness of the diversification strategy published alongside the Bill.
- Additional delays and costs to the roll-out of 5G.[98]

The shadow SNP spokesperson for Business and Industry (Richard Thomson) expressed approval of the Bill, stating that it "provides a very much stronger security framework for telecommunications infrastructure and gives the Government the ability to manage the risk posed by high-risk vendors. I speak on behalf of my group when I say that we support it in all that it is trying to achieve."[99] However, he did call for the inclusion of a duty on the Minister requiring greater consultation with devolved nations on account of the potential for additional costs to devolved governments.[100] This reflects similar concerns raised by SNP members following the July 2020 decision on Huawei.[101]

Dr Julian Lewis, Chair of the Intelligence and Security Committee, welcomed the Bill but criticised the tabling of the Second Reading just four days after the first. He said that the Committee had not had enough time to discuss the contents of the Bill with Government, therefore "our support for the Bill in principle cannot be as unqualified at this stage".[102]

Parliamentary Under-Secretary at DCMS (Matt Warman) closed the debate, responding to some of the concerns raised. He said that the government would work to minimise any further disruption to the 5G roll-out, although he did highlight that decisions made by providers had been "taken at a degree of

[97] HC Deb 30 November 2020 c73
[98] HC Deb 30 November 2020 c79-81
[99] HC Deb 30 November 2020 c84
[100] HC Deb 30 November 2020 c86
[101] HC Deb 14 July 2020 c1387
[102] HC Deb 30 November 2020 c84

commercial risk". He assured that Ofcom would be adequately resourced. With regards to the diversification strategy, he said the following:

> We do not anticipate legislation as a direct result of the diversification strategy, but of course there are other important avenues to explore as part of the broader industrial strategy.[103]

The Bill passed its Second Reading without division.

[103] HC Deb 30 November 2020 c123

8 Committee Stage

The Public Bill Committee met on eight occasions between 14 and 26 January 2021 to consider the Bill. In the first four sittings, it took evidence from representatives of the major telecoms providers, Ofcom and several other key stakeholders, as well as academics. Clause by clause examination of the Bill took place during the final four sittings. The written evidence and transcripts of the Committee's sittings are available on the Telecommunications (Security) Bill 2019-21 page of the Parliament website.

Throughout the proceedings, Matt Warman (Parliamentary Under-Secretary at DCMS) was the Minister speaking on behalf of the Government. The Labour shadow team comprised of Chi Onwurah (Shadow Minister for DCMS), Kevan Jones and Christian Matheson (Shadow Minister for Media). These spokespeople introduced all Opposition amendments during Committee Stage, and **all references to 'the Opposition' in the following section relate to this Labour team.**

All Government amendments were added to the Bill. No Opposition amendments were added. Four Opposition amendments were pushed to division, where they were defeated.

8.1 Opposition amendments

There were three main themes to the Opposition's amendments, as set out by Shadow Minister Chi Onwurah during the debate: national security, diversification of the supply chain and parliamentary scrutiny.[104]

Following the debate, the Minister wrote to Chi Onwurah to further address some of the concerns raised.[105]

National security

The Opposition restated concerns towards DCMS's (and Ofcom's) inexperience in matters of security, with the Shadow Minister stating that "the Department for Digital, Culture, Media and Sport is not known for its understanding of or

[104] PBC Deb, fifth sitting, 21 January 2021, c136-137; PBC Deb, seventh sitting, 26 January 2021, c198

[105] Letter from Matt Warman MP to Chi Onwurah MP and others regarding points raised during the Committee Stage, 26 January 2021

expertise on national security, and we want to take measures to address that."[106] This was a central focus of the Opposition's amendments.

The Minister assured the Committee that "in exercising the powers created by this Bill, the Secretary of State will be advised by the NCSC on relevant technical and national security matters."[107]

5 A definition of national security

During the debate, James Wild (Con) queried why the Opposition had not tabled an amendment to introduce a definition of national security, having highlighted the absence of one as a concern during Second Reading.

The Shadow Minister suggested that the Opposition hoped that a definition of, or minimum standards for, national security would be set out in the National Security and Investment (NS&I) Bill instead, where she argued this would be better placed.[108] The Opposition had introduced an amendment to the NS&I Bill at Committee Stage specifying a range of different factors to consider when assessing a risk to national security, but this was defeated on division.[109] The Labour peer Baroness Hayter of Kentish Town tabled a further amendment to the same Bill which was debated in the Lords at Grand Committee, but not moved any further.[110]

Further information can be found in the Library briefing: National Security and Investment Bill 2019-21, 18 January 2021.

Involvement of intelligence services

A number of Opposition amendments (5, 6, 10, 16 & 17) to **clauses 3 and 15** sought to require consultation with the NCSC and other intelligence services by the Secretary of State when exercising various new powers granted by the Bill. At present, the Bill includes no such requirement.

In response, the Minister said that the department had a good working relationship with the National Cyber Security Centre (NCSC), and that NCSC guidance would form the basis of any codes of practice issued. He argued that the NCSC already has a statutory remit to provide technical security advice and receive security information, therefore this did not need to be included in the Bill.[111] He pointed out that the NCSC was "closely involved" with the drafting of illustrative designation notices published alongside the

[106] PBC Deb, fifth sitting, 21 January 2021, c137

[107] PBC Deb, seventh sitting, 26 January 2021, c222 and c208-209; PBC Deb, sixth sitting, 21 January 2021, c168-169

[108] PBC Deb, fifth sitting, 21 January 2021, c137

[109] PBC Deb, twelfth sitting, 10 December 2020, c350

[110] HL Bill 165 – Running List of Amendments in Grand Committee, 23 February 2021, Amendment 13; HL Deb 2 March 2021 c375GC

[111] PBC Deb, sixth sitting, 21 January 2021, c169

Bill, which he said would be the case for any further designation notices and directions.[112]

The Minister told the Committee that the NCSC and Ofcom will soon publish a joint statement on how they will work together and share information on telecoms security.[113] This was welcomed by Kevan Jones (Lab), although he did question what "legal weight" such a statement would carry and requested that the Minister write to him on this matter.[114]

None of these amendments were pushed to a division.

Ofcom's resourcing

New clauses 3 and 7 were introduced by the Opposition to address concerns regarding Ofcom's resourcing and whether it was sufficient to fulfil its new statutory duties. This issue had previously been raised during Second Reading. It was pointed out that telecoms security was one of several new areas of responsibility that Ofcom had acquired in recent years, despite having no ring-fenced budget. Speaking for the Opposition, Shadow Minister Christian Matheson stated that:

> We heard evidence that Ofcom, in common with other public sector bodies, does not pay as highly as some high-end consultancies, suppliers, developers or software houses, and therefore there will be churn… in terms of Ofcom's ability to maintain its responsibilities in what we know will be a continually evolving sector that throws up new technical challenges.[115]

New clause 3 would require Ofcom to publish an annual report on the adequacy of its budget, funding and staffing levels, and any skills shortages faced. The Shadow Minister explained that:

> The new clause is about assisting Ofcom to make an audit of what is available and ensuring that it is up to standard in terms of technological changes. It will also ensure that it is looking forward, in the midst of all the other responsibilities that Parliament is asking it to undertake, in order to maintain a level of skills and expertise that will enable it to undertake the snapshot reviews of current networks, as well as reviews of future provision and threats to the network.[116]

New clause 7 would require the Secretary of State to lay a report before Parliament on Ofcom's capacity and capability to undertake its new security duties within 12 months of the Bill's passing.

---

[112] PBC Deb, seventh sitting, 26 January 2021, c209

[113] A joint statement has since been published: Ofcom, Joint statement from Ofcom and the National Cyber Security Centre, undated

[114] PBC Deb, sixth sitting, 21 January 2021, c.170

[115] PBC Deb, eighth sitting, 26 January 2021, c233

[116] PBC Deb, eighth sitting, 26 January 2021, c233-234

In response, the Minister pointed out that Ofcom is already required under the Office of Communications Act 2002 to publish an annual report on its finances and other relevant matters. He stated that Ofcom's budget and resources would be increased to meet its new demands under the Bill, but emphasised that Ofcom's responsibilities would lie with the regulation surrounding security issues, rather than making national security decisions. He offered to write to the Intelligence and Security Committee (ISC) (see Box 6 below) to disclose further details about Ofcom's resourcing and security arrangements.[117]

The Shadow Minister welcomed the involvement of the ISC, which he suggested the Minister might bear in mind on Report. He pushed new clause 3 to division, where it was defeated 10 votes to 3.[118] New clause 7 was not moved any further.

Further requirements for network operators

Some probing amendments (7, 8 & 21) to **clause 1** were introduced by the Opposition with the intention of clarifying the duties that the Bill would place on providers.

The Minister assured the Committee that detailed information on how providers would be expected to meet their legal duties would be issued in due course via regulations and codes of practice:

> Ultimately, the new telecoms framework comprises three layers. There are strengthened overarching security duties set out in the Bill, there are specific security requirements in secondary legislation, and there are detailed technical security measures in codes of practice.[119]

He said that this structure was intended to allow the legal framework to be adapted in response to new threats and technological change.[120]

The Minister pointed to draft Electronic Communications (Security Measures) Regulations, published on 13 January 2021, to illustrate how the Government may use its new powers to impose duties on telecoms providers.[121] Concerns have since been raised from within the tech sector towards data retention requirements included in this draft secondary legislation, although criticisms of this nature were not voiced during Committee Stage.[122]

None of these amendments were added to the Bill.

---

[117] PBC Deb, eighth sitting, 26 January 2021, c238-239

[118] PBC Deb, eighth sitting, 26 January 2021, c240

[119] PBC Deb, sixth sitting, 21 January 2021, c167

[120] PBC Deb, sixth sitting, 21 January 2021, c163

[121] PBC Deb, sixth sitting, 21 January 2021, c161

[122] See The New UK Telecoms Security Bill is Starting to Look a Bit Ugly, ISP Review, 16 March 2021; ISPA, ISPA comments on Telecoms Security Bill draft Statutory Instrument, undated

Supply chain diversification

On several occasions, the Opposition stressed the lack of any reference to the diversification strategy in the Bill. Shadow Minister Chi Onwurah highlighted the importance of a diverse supply chain in ensuring overall network resilience and security:

> The dependence of our telecoms security on diversifying the supply chain was set out in the 2019 telecoms supply chain report; yet the Bill fails to mention it at all.[123]

The Shadow Minister said that while the Opposition supported Government efforts to remove high risk vendors from the telecoms network, "those steps must go hand in hand with credible measures to diversify the supply chain, and that must be subject to parliamentary scrutiny". She pointed to a "lack of link" between the diversification strategy and network security and warned that the Bill did not include provisions to mitigate its impact on supply chain diversity.[124]

The Opposition sought to amend the Bill to require Ofcom and the Secretary of State to report directly on the progress of the diversification strategy. Amendment 14 would include an assessment of supply chain diversification as part of Ofcom's security reporting requirements, as set out in **clause 11**. New clause 6 would require the Secretary of State to report annually to Parliament on telecoms supply chain diversity.

In response, the Minister said that the Bill already requires Ofcom's security reports to include information and advice to assist the Secretary of State in the formulation of policy on telecoms security. He argued that this is at Ofcom's discretion, and that diversification does not need to be explicitly mentioned.[125] He added that the Government would be making announcements and providing regular updates on the progress of the diversification strategy "as required".[126]

While the Minister acknowledged the importance of greater diversity, he argued that it "is part of a broader approach to building security and resilience across the global supply chain that sits outside the Bill":

> "The Government cannot legislate for the diversification of the market; that is something that we can incentivise and work with the market to do.
>
> [...]
>
> The focus of the Bill is on setting clear and robust security standards for our networks that telecoms providers must adhere to, and they

[123] PBC, sixth sitting, 21 January 2021, C187
[124] PBC, eighth sitting, 26 January 2021, c246
[125] PBC, seventh sitting, 26 January 2021, c200
[126] PBC, eighth sitting, 26 January 2021, c251-252

> must be met regardless of the diversity within any of those networks. To be fair, the diversity within a provider's supply chain, in and of itself, does not offer the guarantee of network security. A provider using a diverse supply chain needs to be held to the standards set out in this Bill, so that the provider is able to offer the security standards that we need, regardless of the number of suppliers that they have available."[127]

The Shadow Minister suggested that instead of incentivising sufficiently, the Government had "chosen to focus on big sticks for security, as set out in the Bill, such as designations, enforcements and fines of up to 10% of turnover".[128]

The Shadow Minister also criticised the diversification strategy itself as lacking "the clear commitment and funding that one would expect to find in any effective strategy".[129] Similar observations were made by the Science and Technology Committee, which concluded in its February 2021 report on 5G market diversification that the strategy lacked detail and clear milestones. It recommended that the Government publish a more detailed action plan within three months, including "a breakdown of how the initial budget will be spent and a series of milestones with target dates for completion."[130]

Amendment 14 and new clause 6 were both defeated on division.[131]

Parliamentary scrutiny

The Opposition raised concerns towards "the level and extent of appropriate scrutiny for such broad and sweeping powers" afforded by the Bill. Shadow Minister Chi Onwurah suggested that a lack of parliamentary scrutiny had enabled Huawei's continued presence in UK telecoms networks up until the recent Government decision to restrict it (see section 3). She used this to demonstrate the need for effective scrutiny measures to be included in the Bill.[132]

The Opposition recognised that it might not be appropriate to share sensitive security information in Parliament, where it would be in the public domain. Instead, several of its amendments sought to introduce requirements to report to the ISC (see Box 6), thus enabling parliamentary scrutiny.

---

[127] PBC Deb, eighth sitting, 26 January 2021, c251

[128] PBC Deb, eighth sitting, 26 January 2021, c248

[129] PBC Deb, eighth sitting, 26 January 2021, c247

[130] Science and Technology Committee, 5G market diversification and wider lessons for critical and emerging technologies, 4 February 2021, HC 450 2019-21, para 14

[131] PBC Deb, seventh sitting, 26 January 2021, c202; PBC Deb, eighth sitting, 26 January 2021, c253

[132] PBC Deb, seventh sitting, 26 January 2021, c202

6 The Intelligence and Security Committee (ISC)

The Intelligence and Security Committee is the parliamentary committee with statutory responsibility for oversight of the UK Intelligence Community. It also oversees the security related activities of other Government departments and bodies, including the Ministry of Defence, the Cabinet Office and the Home Office. Its members are subject to Section 1(1)(b) of the Official Secrets Act 1989 and are routinely given access to highly classified material in carrying out their duties. See the ISC's website for further information.

Kevan Jones (a Labour member of the ISC) moved amendment 9 to **clause 1** to require the Secretary of State to report information on the specified security measures required of telecoms providers to the ISC. He argued that as the select committee for DCMS does not have the required clearance to scrutinise highly classified evidence, this should be presented to the ISC instead ("the only committee of Parliament that has regular access to protectively marked information that is sensitive for national security reasons").[133]

He assured the Committee that this would be purely for scrutiny purposes, and that:

> the amendment does not propose that the ISC should have a veto or be a regulator, because that would not be correct. Decisions about high-risk vendors are for Ofcom and the Secretary of State.[134]

Similarly, **new clause 5** (tabled by the Opposition) would require the Secretary of State to report annually to the ISC on the impact of designations on national security. Ofcom would also have to report an assessment of future threats to the network and the adequacy of existing security measures.

Shadow Minister Christian Matheson said that presenting information to the ISC for scrutiny was the "right thing" to do.[135]

While recognising the important work undertaken by the ISC, the Minister said in response that it is "important to acknowledge that the ISC is not the only legitimate avenue to scrutinise this framework". He pointed to other parliamentary procedures that would enable scrutiny, including the laying of copies of regulations and codes of practice before Parliament.

He also highlighted the requirement set out in **clause 11** for Ofcom to produce an annual security report which the Secretary of State would be able to publish, as well as the five-yearly review of the framework that would also be

[133] PBC Deb, fifth sitting, 21 January 2021, c145; ISC, Annual Report 2013-14, Annex A, p12
[134] PBC Deb, fifth sitting, 21 January 2021, c143
[135] PBC Deb, fifth sitting, 21 January 2021, c146

laid before Parliament. He offered further assurances that DCMS would continue to engage with the ISC without this being prescribed by the Bill.[136]

Kevan Jones acknowledged DCMS's cooperation, although he cautioned that scrutiny arrangements needed to be included in the Bill in order to "weather the passage of time". He suggested that the Government might want to table a similar amendment of its own at Report stage, before withdrawing amendment 9.[137] New clause 5 was defeated on division, by 10 votes to 3.[138]

Opposition amendments 20 & 22-25 would have required the Secretary of State to present information regarding designated vendor directions and designation notices to the ISC. This was intended to ensure parliamentary oversight of information exempt from being laid before Parliament for national security reasons, in line with **clause 17**.[139]

The Minister pointed out that in exercising the powers granted by the Bill, the Secretary of State will be advised by the NCSC. He argued that as the NCSC's work already falls within ISC's remit, it was unnecessary to include scrutiny provisions in the Bill. [140] None of these amendments were pushed to a division.

8.2 Government amendments

Government amendments 1-4 were added to the Bill. These would cause **clauses 15-23**, and **clause 24** so far as it relates to **clause 18**, to come into force upon Royal Assent, rather than two months after.

[136] PBC Deb, fifth sitting, 21 January 2021, c149
[137] PBC Deb, fifth sitting, 21 January 2021, c150
[138] PBC Deb, eighth sitting, 26 January 2021, c245
[139] PBC Deb, seventh sitting, 26 January 2021, c217
[140] PBC Deb, seventh sitting, 26 January 2021, c222

9 Remaining stages in the Commons

On 30 November 2020, following the Bill's Second Reading, the Government tabled a carry-over motion for the Bill. This was agreed to by the House, enabling the Bill to continue its progress into the next parliamentary session. The remaining stages in the Commons (Report and Third Reading) took place on 25 May 2021.[141]

Three new clauses were pushed to division at Report Stage by the Labour Opposition, but all of them were defeated (and not added to the Bill)[142]:

- **New Clause 1** would have required Ofcom to report annually on the adequacy of its resources and to assess the adequacy of the measures taken by telecoms providers to comply with their security duties. It would also have required Ofcom to assess future areas of security risk based on its interrogation of network providers' asset registries.

- **New Clause 2** would have required the Secretary of State to provide the Intelligence and Security Committee of Parliament with information relating to a designated vendor direction, notification of contravention, urgent enforcement action or modifications to an enforcement direction made on grounds of national security "as soon as is reasonably practicable".

- **New Clause 3** would have required the Secretary of State to report annually on the impact of the Government's diversification strategy on the security of telecoms networks and services, and allow for a debate on the report in the House of Commons.

The SNP tabled a further amendment (to **clause 14)** which would have required the Secretary of State to consult with appropriate ministers in the devolved governments when conducting the five-yearly review of the impact and effectiveness of clauses 1 to 13 of the Bill. This amendment was not moved any further.

Third Reading followed the Report Stage debate. The Bill was not amended and passed this stage without division.[143]

[141] HC Deb 25 May 2021 c278-328

[142] UK Parliament, Votes and Proceedings: Tuesday 25 May 2021, Item 5

[143] HC Deb 25 May 2021 c324-328

10 House of Lords stages

The House of Lords Library produced a briefing for Lords stages: Telecommunications (Security) Bill: Briefing for Lords Stages.

The Bill was introduced to the House of Lords as HL Bill 15 2021-22 and had its First Reading on 26 May 2021. Second Reading followed on 29 June, which the Bill passed without division.[144] It was then debated in Grand Committee over two sittings on 13 and 15 July. A range of amendments were considered but none were added to the Bill.[145]

Report stage in the Lords took place on 19 October. Five amendments were agreed (discussed in further detail below). Lords Third Reading was held on 26 October, which it passed without division.[146]

The Bill now returns to the Commons on Monday 8 November 2021 for consideration of Lords amendments.

10.1 Amendments at Report Stage

During Report Stage in the Lords, five amendments were agreed which would bring effect to three substantive changes to the Bill. One was a Government amendment relating to the procedure for issuing codes of practice. The other two were non-Government amendments, relating to network diversification and the review of telecoms companies that have been banned by Five Eyes partners.

Codes of practice about security measures, etc.

The Government introduced amendments 3-5 to **clause 3**, which provides the Secretary of State with the power to issue codes of practice.

Lords Amendment 3 (listed as **Amendment 1** as the Bill returns to the Commons) would apply a negative resolution procedure to this power, providing Parliament with a 40-day period in which it could choose not to approve the issuing of the draft code. Amendment 4 is a consequential technical amendment to the clause and Amendment 5 inserts a definition of the "40-day period".

[144] HL Deb 29 June 2021 c706-751

[145] HL Deb 13 July 2021 c459-51bGC; HL Deb 15 July 2021 c519-565GC

[146] HL Deb 26 October 2021 c646-649

The Delegated Powers and Regulatory Reform Committee had previously highlighted the "significance of the statutory effects" of the codes of practice and recommended that the application of the negative procedure would afford an "appropriate level" of parliamentary scrutiny over this.[147]

Initially, the Government rejected this on the grounds that the Bill already provided for sufficient scrutiny.[148] However, it later accepted this recommendation and tabled an amendment at Lords Report Stage to enact it. It provided the following explanation in a letter to the Chair of the Committee':

> The codes of practice are technical in nature and are one part of a framework which is tailored to be appropriate and proportionate to the risks it addresses. They will detail practical security measures relating to specific technology. Their intended audience is security professionals working for public telecoms providers. We need the codes to be able to be understood by that audience. They are not intended to be formal pieces of secondary legislation. Therefore, the Office of Parliamentary Counsel has advised that we can amend the Bill in a way that applies the negative procedure to the issuing of codes of practice, without placing the code itself into a statutory instrument. This will provide Parliament with the opportunity to scrutinise any code of practice, ensuring the recommendations of the Committee and the concerns raised during debates in the House of Lords are addressed.[149]

The amendments were agreed by the House without debate.[150]

Network diversification

Lords Amendment 8, moved by Baroness Merron (Lab), inserts a new clause after **clause 23** that would require the Secretary of State to report annually on the impact of the Government's diversification strategy on the security of telecommunications networks and services. The amendment would require the report to be laid before Parliament and allow for a debate in the House of Commons on the report. The same amendment had previously been debated at Lords Committee Stage.[151]

This new clause was opposed by the Government, but was agreed by the Lords on division (180 to 176 votes).[152] It returns to the Commons as **Lords Amendment 4**.

Throughout consideration of the Bill, in both the Commons and Lords, Oppositions Members have highlighted the lack of any reference to the

[147] Delegated Powers and Regulatory Reform Committee, 4th Report, 24 June 2021, HL 29, para 27 & 36
[148] Delegated Powers and Regulatory Reform Committee, 5th Report, 20 June 2021, HL 48, Appendix 2
[149] Delegated Powers and Regulatory Reform Committee, 9th Report, 21 October 2021, HL 83, Appendix 1
[150] HL Deb 19 October 2021 c81
[151] HL Deb 15 July 2021 c546-553GC
[152] HL Deb 19 October 2021 c90

diversification strategy in the Bill (see section 8.1: supply chain diversification for discussion). Again, Baroness Merron stressed the importance of supply chain diversity:

> As we heard in Committee, there is wide cross-party support for the principle that our networks will not be secure if the supply chain is not diversified. For me, this is at the very heart of the Bill and what it should seek to address. Unfortunately, we still have a Bill that seeks to secure telecoms security yet seems to think it is possible to be silent on diversification. Even though the former Minister said in Committee that
>
> "diversification is designed to enhance security and resilience",—[*Official Report*, 15/7/21; col. GC 551.]
>
> the Government have said that this amendment is not appropriate. The importance of the amendment could not be clearer. I remind noble Lords that, once Huawei is removed, the UK will be left with effectively only two service providers. This is a matter of the highest concern. We need and must have a diversified supply chain. That means diversity of supply at different points in the supply chain and that different networks do not all share the same vulnerabilities of a particular supplier. This is absolutely crucial for network resilience. It will also support British companies and grow British jobs.
>
> If the Government fail to amend the Bill on this point by accepting this amendment, they are putting our national security at risk.[153]

Lord Parkinson of Whitley Bay (Minister for Arts at DCMS) responded by saying that the Bill was not the right place for this amendment for two reasons:

1. Diversification extends well beyond the security focus of the Bill – work currently underway is also aimed at boosting quality, innovation, competition and choice within telecoms networks.
2. Legislating for a reporting requirement would be limiting and inflexible as the Government's diversification work evolves.[154]

He went on to offer reassurances that the Government's work on diversification is progressing "at pace".[155]

Review of telecoms companies based in foreign countries

Lord Alton of Liverpool (a crossbench peer) moved Amendment 11 (**Amendment 5** as the Bill returns to the Commons). This inserts a new clause that would amend the Communications Act 2003 to require the Secretary of

[153] HL Deb 19 October 2021 c85
[154] HL Deb 19 October 2021 c86
[155] HL Deb 19 October 2021 c87

State to review decisions taken by Five Eyes partners (the US, Canada, Australia and New Zealand) to ban telecoms vendors on security grounds. This would involve reviewing the UK's security arrangements with that vendor and considering whether to issue a designated vendor direction or take similar action. A similar amendment was also debated at Lords Committee Stage.[156]

Lord Alton emphasised the UK's relationship with its Five Eyes partners and argued that this amendment would "strengthen international action and bolster UK resilience and security". He suggested that if such a provision had previously existed in UK law, it might have saved the country a "great deal of money" over the Huawei 5G "debacle".[157]

In response, the Minister agreed it was important that the UK Government should engage with international partners, but noted that mechanisms for this already existed. As such, he suggested that this amendment was not necessary. The Minister also pointed to **clause 16** of the Bill, which sets out a non-exhaustive list of factors the Secretary of State might take into account when considering whether to issue a designation notice.[158]

This new clause was opposed by the Government, but was agreed by the Lords on division (172 to 156 votes).[159]

[156] HL Deb 13 July 2021 c460
[157] HL Deb 19 October 2021 c98
[158] HL Deb 19 October 2021 c103-4
[159] HL Deb 19 October 2021 c107

The House of Commons Library is a research and information service based in the UK Parliament. Our impartial analysis, statistical research and resources help MPs and their staff scrutinise legislation, develop policy, and support constituents.

Our published material is available to everyone on commonslibrary.parliament.uk.

Get our latest research delivered straight to your inbox. Subscribe at commonslibrary.parliament.uk/subscribe or scan the code below:

commonslibrary.parliament.uk

@commonslibrary