ALLEN & OVERY

The Telecommunications (Security) Bill: the rollercoaster ride continues

On 24 November 2020, the Telecommunications (Security) Bill (the **Bill**) was introduced by the UK Government into Parliament. As anticipated, the Bill seeks to introduce a new regulatory framework for telecommunications security in the UK, particularly in the light of concerns raised by the UK Government on the involvement of Chinese technology company, Huawei, in the UK's telecoms infrastructure.

The Bill would place stronger security-related duties and responsibilities on telecoms companies and would grant Ofcom, the UK's communications regulator, new enforcement powers. Additionally, and building on the UK Government's previous announcements in relation to so-called "high risk vendors" (**HRVs**), the Bill would give the Secretary of State powers to impose directions on "public communications providers" (**Providers**)[1] in relation to HRVs, which the Bill refers to as "designated vendors".

The Bill was accompanied by a roadmap relating to the removal of HRVs from the UK's telecoms network (the **Roadmap**) and a 5G supply chain diversification strategy (the **Strategy**). In this article, we examine the key features of the Bill relating to "designated vendors", the Roadmap and the Strategy.

The background to the Bill

The Bill comes after a period of considerable uncertainty surrounding the UK's policy towards HRVs and telecoms security issues more generally. The UK's Secretary of State for Digital, Culture, Media and Sport, Oliver Dowden, has stated that the Bill is intended to "give the UK one of the toughest telecoms security regimes in the world".[2]

The policy background to the Bill is set out in our recent publication: **The UK Government reverses its approach to high risk vendors in telecoms**. Importantly, it comes at a time when the UK is conducting a major upgrade of its digital infrastructure[3] against a backdrop of an increase in cyber-security threats.[4]

A two-stage process: "designation notices" and "designated vendor directions"

In relation to "designated vendors", the Bill would create new national security-related powers through the insertion of new provisions into the Communications Act 2003, which sets out the current regulatory framework for the telecommunications sector in the UK. A two-stage process is envisaged by the Bill. First, the Secretary of State would designate a person as a "designated vendor" by issuing a "designation notice" (a **Notice**).

This would then give the Secretary of State the power to give directions to Providers through a "designated vendor direction" (a **Direction**) regarding how Providers can use the "designated vendor". Importantly, neither a Notice nor a Direction require Parliamentary approval. Both must be laid before Parliament, though not if the Secretary of Security considers that such a step would be contrary to the interests of national security.

The Bill provides that a Notice can only be issued if the Secretary of State considers that the Notice is "necessary in the interests of national security". The Secretary of State, in making a decision, may have regard to a range of factors relating to the person being considered for designation including the:

- nature of the goods, services or facilities that are or might be supplied, provided or made available by the person;
- quality, reliability and security of those goods, services or facilities or any component of them (including the quality, reliability and security of their development or production or of the manner in which they are supplied, provided or made available);
- reliability of the supply of those goods, services or facilities;
- quality and reliability of the provision of maintenance or support for those goods, services or facilities;
- extent to which and the manner in which goods, services or facilities supplied, provided or made available by the person are or might be used in the UK; and
- extent to which, and the manner in which goods, services or facilities supplied, provided or made available by the person are or might be used in other countries or territories.

Importantly, the identity of the person under consideration for designation, including the country or territory of their registered office, the identity of the persons who own or control them and the degree to which any of those persons might be susceptible to being influenced or required to act contrary to the interests of the UK's national security, will be taken into consideration. Supply chains will also be considered as the indicative factors include the identity of the persons concerned in the development, production and supply of goods, services and facilities, as well as persons providing associated maintenance or support. As "national security" is undefined and the list of factors is wide-ranging and non-exhaustive, the Secretary of State will have considerable latitude when deciding to issue Notices.

Prior to a Notice being issued, the Secretary of State is required to consult the person or persons named on the Notice, as far as it is reasonably practicable to do so, unless that consultation would be contrary to the interests of national security. Notices can be varied or revoked.

Once a Notice has been issued, the Secretary of State may give a Direction to a Provider. Such a Direction can only be given if the Secretary of State considers that the Direction is necessary in the interests of national security and the requirements imposed by the Direction are proportionate to what is sought to be achieved by it. The Direction may impose requirements on the use of goods, services or facilities that are supplied, provided or made available by the "designated vendor". For example, the requirements could impose a prohibition or restriction on the use of goods, services or facilities provided or made available by the "designated vendor", requirements to modify such services, or requirements about the way in which such goods, services or facilities may be used.

In short, the power envisaged in the Bill relating to the content of a Direction is wide-ranging and confers considerable discretion on the Secretary of State.

Before a Direction is given, the Secretary of State must consult the Provider(s) that would be subject to the proposed Direction and the relevant "designated vendor", as far as it is reasonably practicable to do so, unless that consultation would be contrary to the interests of national security. A Provider is required to comply with a Direction and Directions can be varied or revoked.

An illustrative Notice and Direction have been published in relation to Huawei which reflect the matters on which the Secretary of State "is presently minded to consult **Huawei** and public communication providers upon the enactment of the Bill".[5]

The Bill also gives the Secretary of State the power to require a Provider to produce a plan setting out the steps it intends to take to ensure compliance with a Direction and the timing of those steps (a **Compliance Plan**). The Secretary of State will have the power to specify the period within which a plan must be provided to Ofcom and the Secretary of State.

Monitoring, enforcement and non-disclosure requirements

The Bill gives powers to the Secretary of State and Ofcom to monitor implementation of Directions, backed up by a maximum penalty of GBP10 million, or GBP50,000 per day in cases of continued contravention, in the case of non-compliance with the monitoring regime by Providers.

The Bill also provides the Secretary of State with the power to require information from relevant persons to support the Government's monitoring efforts and decision making. A notice is required in relation to such requests and contravention of that notice carries a maximum penalty of GBP10m, or GBP50,000 per day in cases of continued contravention.

The Bill contains robust enforcement provisions that allow the Secretary of State to determine that a Provider is contravening, or has contravened, a requirement in a Direction or a requirement in relation to a Compliance Plan. In such circumstances, the Secretary of State can issue a notice of contravention which specifies the remedial steps required of the Provider and the penalty that the Secretary of State is minded to impose.

That penalty must be appropriate and proportionate to the contravention in respect of which it is imposed. Where a Direction is said to have been contravened, the maximum value of the penalty is 10% of the Provider's relevant turnover during a specified period or GBP100,000 per day in respect of a continuing contravention. In the case of a contravention of a Compliance Plan, it is GBP10m, or GBP50,000 per day. It is clear that the penalties for breaching a Direction are intended to have a deterrent effect and the UK Government has stated that it will take a "robust" approach to monitoring compliance.[6]

Before a notice of contravention is finalised through the issuance of a "confirmation decision", the Secretary of State must allow the Provider to make representations. Once the period for those representations has passed, the Secretary of State may decide not to take any furtheraction or to issue a "confirmation decision". A "confirmation decision" must be provided without delay, include reasons and may require immediate remedial actions to be taken and/or the payment of a penalty. A Provider would be placed under a duty to comply with the "confirmation decision" which is enforceable in civil proceedings.

Furthermore, the Bill provides the Secretary of State with powers to give an "urgent enforcement direction". Such a direction could be given in circumstances where, for example, the Secretary of State determines that there are reasonable grounds for believing that a Provider is contravening, or has contravened, a requirement imposed by a "designated vendor direction", the contravention has resulted in, or creates a risk of, a serious threat to national security and it is appropriate for the Secretary of State to take action. The "urgent enforcement direction" will specify the steps that the recipient is required to take to comply with the requirement or remedy the consequences of the contravention. A recipient of an "urgent enforcement direction" would have a duty to comply which is enforceable in civil proceedings.

Finally, in relation to "designated vendors", the Bill provides the Secretary of State with powers to require the non-disclosure of the existence or content of certain documents and consultations where their disclosure is determined to be contrary to national security. The penalties for non-compliance with the non-disclosure obligations are a maximum penalty of GBP10m, or GBP50,000 per day in cases of continued contravention.

The Roadmap and the Strategy

The Roadmap and the Strategy were published shortly after the Bill. Together they set out the UK Government's approach to expediting the removal of Huawei's equipment from the UK's 5G network and ensuring that the UK does not become, in Huawei's absence, overly reliant on any other suppliers. Two important elements announced in the Roadmap and the Strategy are that the installation of any of Huawei's equipment in the UK's 5G network will be prohibited from the end of September 2021 and GBP250m has been pledged to create a "more diverse, competitive, and innovative supply market for telecoms".[7] This money will be spent on a number of projects including funding a new Open RAN trial with NEC (a Japanese telecoms vendor) and establishing a National Telecoms Lab. Additionally, the UK Government will prioritise influencing standard-setting bodies and taking a leadership role internationally to establish a competitive and sustainable supply chain.

Conclusion

The Bill's powers in relation to "designated vendors" represent a watershed moment in the development of the UK's response to cyber-security threats and national security concerns in relation to the UK's telecommunications network. Notably, the powers envisaged are exceptionally broad, afford considerable discretion to the Secretary of State and are subject to limited Parliamentary oversight. Certainly, we expect the latter point will be a particular focus of debate during the Bill's Parliamentary passage. Industry participants will also no doubt be concerned about the breadth of the requirements that can be imposed, the potentially invasive nature of the UK Government's monitoring powers and the level of due diligence that they may be required to engage in to assess the risks associated with their supply chains.

The Bill has also been introduced at a time when the **National Security and Investment Bill** is being debated in Parliament. Taken together, these bills create a formidable armoury of new powers for the UK Government to intervene in the operation of the UK's telecommunications sector. All businesses operating in the sector will need to consider carefully the potential impact of the bills on their activities. We expect both bills to come into force in the first quarter of 2021.

Authors

Matthew Townsend
Partner – London
Tel +44 20 3088 3174
matthew.townsend@allenovery.com

Jonathan Benson
Senior Associate, London
Tel +44 20 3088 1321
jonathan.benson@allenovery.com

1. These includes companies such as BT, Vodafone and Virgin Media that provide networks and/or services that are wholly or mainly used by the public.
2. See **here**.
3. See **here**.
4. See, for example, **GCHQ's characterisation of the cyber threat**, the UK's **National Cyber Security Strategy** and various UK National Cyber Security Centre reports in relation to cyber threats from **Russia** and **China**.
5. See **here**.
6. See **here**.
7. See **here**.

UK
CS2012_CDD-62314_ADD-93412