# New telecoms security law to protect UK from cyber threats

- New legal duties on telecoms firms to increase the security of entire UK network
- New powers for government to remove high risk vendors such as Huawei
- New responsibilities on Ofcom to monitor telecoms operators' security
- Fines up to ten per cent of turnover or £100,000 a day for failing to meet standards

The Telecommunications (Security) Bill aims to give the government unprecedented new powers to boost the security standards of the UK's telecoms networks and remove the threat of high risk vendors.

The Bill will strengthen the security framework for technology used in 5G and full fibre networks including the electronic equipment and software at phone mast sites and in telephone exchanges which handle internet traffic and telephone calls.

This will be a significant step to protect the UK from hostile cyber activity by state actors or criminals. Over the past two years the Government has attributed a range of cyber attacks to Russia and China, as well as North Korea and Iranian actors.

The Bill will also provide the Government with new national security powers to issue directions to public telecoms providers in order to manage the risk of high risk vendors. While they are already banned from the most sensitive 'core' parts of the network, the Bill will allow the Government to impose controls on telecoms providers' use of goods, services or facilities supplied by high risk vendors.

Companies which fall short of the new duties or do not follow directions on the use of high risk vendors could face heavy fines of up to ten per cent of turnover or, in the case of a continuing contravention, £100,000 per day. Ofcom will be given the duty of monitoring and assessing the security of telecoms providers.

In July, following advice from the National Cyber Security Centre (NCSC), the government announced new controls on the use of Huawei 5G equipment – including a ban on the purchase of new Huawei equipment from the end of this year and a commitment to remove all Huawei equipment from 5G networks by 2027. The Bill creates the powers that will allow the government to enshrine those decisions in law and manage risks from other high risk vendors in the future.

**Digital Secretary Oliver Dowden said:**

> We are investing billions to roll out 5G and gigabit broadband

> across the country, but the benefits can only be realised if we have full confidence in the security and resilience of our networks.

“This groundbreaking bill will give the UK one of the toughest telecoms security regimes in the world and allow us to take the action necessary to protect our networks.”

Currently, telecoms providers are responsible by law for setting their own security standards in their networks. However, the Telecoms Supply Chain Review concluded by the government last year found providers often have little incentive to adopt the best security practices.

To deliver the revolutionary economic and social benefits of 5G and gigabit-capable broadband connections, the government has decided to strengthen the overarching legal duties on providers of UK public telecoms networks and services as a way of incentivising better security practices.

These duties will be set out in the Bill and will mean telecoms providers will need to take appropriate action to bring in minimum security standards for their networks and services and to limit the damage of any breaches.

The Bill will allow the government to issue specific security requirements that providers will need to follow to meet these duties. These requirements will be set out in secondary legislation, but are likely to involve companies acting to:

- securely design, build and maintain sensitive equipment in the core of providers’ networks which controls how they are managed;
- reduce the risks that equipment supplied by third parties in the telecoms supply chain is unreliable or could be used to facilitate cyber attacks;
- carefully control who has permission to access sensitive core network equipment on site as well as the software that manages networks;
- make sure they are able to carry out security audits and put governance in place to understand the risks facing their public networks and services; and
- keep networks running for customers and free from interference, while ensuring confidential customer data is protected when it is sent between different parts of the network.

New codes of practice will demonstrate how certain providers should comply with their legal obligations. These will be published once the Bill has received Royal Assent.

Telecoms watchdog Ofcom will be given stronger powers to monitor and assess operators’ security, alongside enforcing compliance with the new law. This will include carrying out technical testing, interviewing staff, and entering operators’ premises to view equipment and documents.

Markets across the world have become overly reliant on too few vendors due to a lack of competition in the global telecoms supply chain. The government has

been engaging extensively with operators, vendors and governments around the world and will soon publish its 5G Diversification Strategy to address this head-on. The strategy will outline new measures to boost competition and innovation in the telecoms supply chain and reduce dependence on individual suppliers.

**NCSC Technical Director Dr Ian Levy said:**

> The roll-out of 5G and gigabit broadband presents great opportunities for the UK, but as we benefit from these we need to improve security in our national networks and operators need to know what is expected of them.

“We are committed to driving up standards and this bill imposes new telecoms security requirements, which will help operators make better risk management decisions.”

**ENDS**

Notes to Editors

- Protecting the UK’s telecoms networks has always been the government’s top priority. In January, the government concluded high risk vendors should be excluded from the core and most sensitive parts of the UK’s 5G network, restricted to up to a 35 per cent market share in the access network (subject to an NCSC approved mitigation strategy), which connects devices and equipment to mobile phone masts, by 2023, with the decisions kept under review. Our word-leading cyber security experts were satisfied that with our approach and tough regulatory regime, any risk can be safely managed, but were also clear that further sanctions could require them to change that assessment.
- In July, in response to US sanctions against Huawei, the DCMS Secretary of State announced the complete removal of Huawei equipment from our 5G networks by the end of 2027. Since Huawei first came to the UK in 2003, their presence has been carefully risk-managed. Huawei’s current presence in the UK is subject to detailed formal oversight through the Huawei Cyber Security Evaluation Centre since 2010, and the HCSEC Oversight Board, which has reported annually since 2014.
- Examples of the cyber attacks or breaches the Telecoms (Security) Bill will help to guard the UK against include: 1) Espionage attacks on networks which happen because of the poor security of the companies that provide equipment support to telecoms providers. In 2018, the Chinese ‘APT 10’ group attack on global networks, also known as ‘Cloudhopper’, targeted a range of companies, including in aerospace and defence, telecommunications, professional services, utility sectors and many more. It was one of the most significant and widespread cyber intrusions against the UK and allies uncovered to date targeting trade secrets and economies around the world. 2) Networks being remotely disabled because of insecure connections to other networks, which has caused mobile outages in other countries. This happened in 2016 when unusual network

traffic was received by Norwegian telecoms provider Telenor, causing an outage which impacted up to three million customers for 18 hours.

- The government will consult with industry on the new framework before secondary legislation is laid in Parliament. The government will launch a public consultation on the codes of practice after the Bill’s passage to ensure those affected can put forward views on which companies should be subject to new technical requirements and how quickly this work should be carried out.
- Ofcom will also be given a new power to direct telecoms providers to take interim steps to address security gaps during the enforcement process and it will take the Codes of Practice into account when carrying out its role.
- The DCMS Secretary of State will have powers to enforce compliance with designated vendor directions, including through fines, and can ask Ofcom to inspect and investigate and provide compliance reports to the government.