Huawei legal notices issued

Huawei technology must be removed from the UK's 5G public networks by the end of 2027 under legal documents handed to broadband and mobile operators today.

The document – called a designated vendor direction – has been sent to 35 UK telecoms network operators. It puts the government's previous position to remove Huawei kit from UK 5G networks on a legal footing.

The ban on Huawei in 5G follows guidance from the world leading National Cyber Security Centre (NCSC) that the security of the company's products – such as equipment used at phone mast sites and telephone exchanges – can no longer be managed due to the impact of US sanctions on its supply chain. The sanctions, imposed by the US Government in 2020, stop Huawei accessing US semiconductor technology on which it previously relied.

Huawei has been issued a separate document – a designation notice – which categorises the company as a high-risk vendor of 5G network equipment and services. The designation notice sets out all of the reasons for which the government considers Huawei to pose a national security risk, including the impact of the sanctions.

The direction sets out the controls to be placed on operators' use of Huawei, following consultation with Huawei and telecoms operators, including:

- an immediate ban on the installation of new Huawei equipment in 5G networks;
- a requirement to remove Huawei equipment from 5G networks by the end of 2027;
- a requirement to remove Huawei equipment from the network core by 31 December 2023;
- a requirement to limit Huawei to 35 per cent of the full fibre access network by 31 October 2023;
- a requirement to remove Huawei equipment from sites significant to national security by 28 January 2023; and
- a requirement not to install any Huawei equipment that has been affected by US sanctions in full fibre networks.

These decisions have been reached following technical security analysis from the National Cyber Security Centre which takes into account our specific national circumstances and how the risks from the US sanctions are manifested in the UK. The decisions will not cause any delays to the government's digital infrastructure roll out targets.

Having fully considered consultation responses, the key deadline to remove all Huawei equipment in the UK's 5G network by 2027 remains unchanged, as do eight of the other interim deadlines to guide operators in meeting the 2027 deadline.

For a small number of operators, the two interim deadlines for the core and

35 per cent of the full fibre access network could have led to network outages and disruption for customers, due to delays caused by the pandemic and global supply chain issues.

Having considered comments raised by industry in the consultation, the government has formally set interim deadlines that balance the need to remove Huawei as swiftly as possible while avoiding unnecessary instability in networks. The UK's world-leading cyber security experts at the NCSC have agreed this is a sensible balance.

Providers should meet the original target dates for the removal of Huawei from network cores and capping Huawei at 35 per cent in the access network (January and July 2023 respectively) wherever possible, and the government expects most of them will do so.

Digital Secretary Michelle Donelan said:

"We must have confidence in the security of our phone and internet networks which underpin so much about our economy and everyday lives.

"Thanks to this government's tough new laws we can drive up the security of telecoms infrastructure and control the use of high-risk equipment.

"Today I'm using these powers and making it a legal requirement for Huawei to be removed from 5G networks by 2027."

NCSC Technical Director Dr Ian Levy said:

"Society increasingly relies on telecoms and the NCSC, government and industry partners work closely to help ensure that these networks are secure and resilient in the long term.

"The Telecoms Security Act ensures we can be confident in the resilience of the everyday services on which we rely, and the legal requirements in this Designated Vendor Direction are a key part of the security journey."

The decision comes as the government publishes its response to a targeted consultation on a proposed ban held earlier this year with Huawei and other telecoms companies under the provisions of the Telecommunications (Security) Act 2021.

The Act came into force in November last year and gives the government new powers to control the presence of high risk vendors in UK public telecoms networks where necessary in the interests of national security.

Separately, last month the government introduced tough new security rules broadband and mobile companies will have to follow to better protect UK networks from potential cyber attacks under the Telecommunications (Security) Act.

The new regulations and code of practice are among the strongest in the world and provide much tougher protections for the UK from cyber threats which could cause network failure or the theft of sensitive data.

Ofcom will oversee, monitor and enforce the new regulations and code and have the power to carry out inspections of telecoms firms' premises and systems to ensure they're meeting their obligations. If companies fail to meet their duties, the regulator will be able to issue fines of up to 10 per cent of turnover or, in the case of a continuing contravention, £100,000 per day.

ENDS

Notes to editors

In 2020 the NCSC published updated guidance in relation to Huawei. It has also published a number of other documents:

- A summary of the NCSC's analysis of the May 2020 US sanction of Huawei
- A blog: 'A different future for telecoms in the UK'
- An explainer: Why has the NCSC's advice on the use of Huawei technology changed?
- An explainer: What is 5G, and how will it affect you