35th Universal Periodic Review: UK statement on Turkey

The Universal Periodic Review takes place in Geneva.

The United Kingdom notes that the end of the state of emergency following the 2016 failed coup, and progress against Daesh and the PKK, provide opportunity for reform ahead of the 2023 elections.

We are concerned by harassment and imprisonment of journalists. We trust the Government will remove obstacles to freedom of expression.

We recommend that Turkey:

1. Implement the National Action Plan and Strategy Document on Combating Child, Early and Forced Marriages.
2. Protect freedom of expression, including for journalists and human rights defenders, by decriminalising defamation.
3. Amend constitutional provisions on appointing members of the Council of Judges and Prosecutors, ensuring their peers elect the majority.

Published 28 January 2020

Baroness Morgan's Written Ministerial Statement to the House of Lords on UK Telecommunications

UK TELECOMMUNICATIONS

The Telecoms Supply Chain Review – laid before Parliament in July 2019 – underlined the range and nature of the risks facing our critical digital

infrastructure.

The Review addressed three questions:

*How should telecoms operators be incentivised to improve security standards and practices in 5G and full fibre networks? * How should the security challenges posed by high risk vendors be addressed? * How can sustainable diversity in the telecoms supply chain be created?

The Government is establishing one of the strongest regimes for telecoms security in the world. This will raise security standards across the UK's telecoms operators and the vendors that supply them. At the heart of the new regime, will be the National Cyber Security Centre's Telecoms Security Requirements guidance. This will raise the height of the security bar and set out tough new standards to be met in the design and operation of the UK's telecoms networks.

The Government intends to legislate, at the earliest opportunity, to introduce a new comprehensive telecoms security regime – to be overseen by the communications sector regulator, Ofcom, and Government.

The Review also underlined the need for the UK to improve diversity in the supply of equipment to telecoms networks.

The Government is developing an ambitious strategy to help diversify the supply chain. This will entail the deployment of all the tools at the Government's disposal. The strategy has three main strands:

- Attracting established vendors who are not currently present in the UK;
- Supporting the emergence of new, disruptive entrants to the supply chain; and
- Promoting the adoption of open, interoperable standards that will reduce barriers to entry.

The UK's telecoms operators are leading the world in the adoption of new, innovative approaches to expand the supply chain. The Government will work with industry and like-minded countries to achieve these goals.

The third area covered by the Review was how to treat those vendors which pose greater security and resilience risks to UK telecoms.

The Government has now completed its consideration of all the information and analysis on this subject, and is publishing the final conclusions of the Telecoms Supply Chain Review in relation to high risk vendors.

In order to assess a vendor as high risk, the Review recommends a set of objective factors are taken into account. These include:

- the strategic position or scale of the vendor in the UK network;
- 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;
- the vendor’s domestic security laws in the jurisdiction where the vendor is based and the risk of external direction that conflicts with UK law;
- the relationship between the vendor and the vendor’s domestic state apparatus; and
- the availability of offensive cyber capability by that domestic state apparatus, or associated actors, that might be used to target UK interests.

To ensure the security of 5G and full fibre networks, it is both necessary and proportionate to place tight restrictions on the presence of any vendors that are identified as higher risk.

For 5G and full fibre networks, the Review concluded that, based on the current position of the UK market, high risk vendors should be:

- Excluded from all safety related and safety critical networks in Critical National Infrastructure;
- Excluded from security critical network functions;
- Limited to a minority presence in other network functions to a cap of up to 35%; and
- Subjected to tight restrictions, including exclusions from sensitive geographic locations.

These new controls will also be contingent on an NCSC-approved risk mitigation strategy for any operator using such a vendor.

The Government intends to bring forward legislation, at the earliest opportunity, to limit and control the presence of high risk vendors in UK networks, and to be able to respond appropriately as technology changes.

Nothing in the Review’s conclusions affects this country’s ability to share highly sensitive intelligence data over highly secure networks, both within the U.K. and with our partners, including the Five Eyes.

GCHQ have categorically confirmed that how the UK constructs its 5G and full fibre public telecoms networks has nothing to do with how the Government shares classified data.

In response to the Review, the Government has asked the National Cyber Security Centre to produce guidance for industry in relation to high risk vendors. The guidance sets out how NCSC will determine whether a vendor is high risk, the precise restrictions it advises should be applied to high risk vendors in the UK’s 5G and full fibre networks, and what mitigation measures operators should take if using high risk vendors.

The NCSC has published that guidance on their website at: www.ncsc.gov.uk/guidance/ncsc-advice-on-the-use-of-equipment-from-high-risk-vendors-in-uk-telecoms-networks, as well as a summary of the security analysis conducted for the Telecoms Supply Chain Review at: [www.ncsc.gov.uk/report/summary-of-NCSC-security-analysis-for-the-UK-telecoms

-sector]. The DCMS press release accompanying this Written Ministerial Statement can be found at: https://www.gov.uk/government/news/new-plans-to-safeguard-countrys-telecoms-network-and-pave-way-for-fast-reliable-and-secure-connectivity.

Copies of these documents have been placed in the House of Commons library.

-END-

New plans to safeguard country's telecoms network and pave way for fast, reliable and secure connectivity

- High risk vendors to be excluded from sensitive 'core' parts of 5G and gigabit-capable networks
- 35 per cent cap on high risk vendor access to non-sensitive parts of the network
- NCSC issues guidance to operators on implementing decision with legislation introduced at the earliest opportunity

Ministers today determined that UK operators should put in place additional safeguards and exclude high risk vendors from parts of the telecoms network that are critical to security.

High risk vendors are those who pose greater security and resilience risks to UK telecoms networks.

The Prime Minister chaired a meeting of the National Security Council (NSC), where it was agreed that the National Cyber Security Centre (NCSC) should issue guidance to UK Telecoms operators on high risk vendors following the conclusions of the Telecoms Supply Chain Review.

This advice is that high risk vendors should be:

- Excluded from all safety related and safety critical networks in Critical National Infrastructure
- Excluded from security critical 'core' functions, the sensitive part of the network
- Excluded from sensitive geographic locations, such as nuclear sites and military bases
- Limited to a minority presence of no more than 35 per cent in the periphery of the network, known as the access network, which connect devices and equipment to mobile phone masts

As part of the Review, the NCSC carried out a technical and security analysis

that offers the most detailed assessment in the world of what is needed to protect the UK's digital infrastructure.

The guidance sets out the practical steps operators should take to implement the government's decision on how to best mitigate the risks of high risk vendors in 5G and gigabit-capable networks.

The government will now seek to legislate at the earliest opportunity to put in place the powers necessary to implement this tough new telecoms security framework.

The government is certain that these measures, taken together, will allow us to mitigate the potential risk posed by the supply chain and to combat the range of threats, whether cyber criminals, or state sponsored attacks.

The Review also highlighted the need for the UK to improve the diversity in the supply of equipment to telecoms networks.

The government is now developing an ambitious strategy to help diversify the supply chain. This will seek to attract established vendors who are not present in the UK, supporting the emergence of new, disruptive entrants to the supply chain, and promoting the adoption of open, interoperable standards that will reduce barriers to entry.

The recommended cap of 35 per cent will be kept under review to determine whether it should be further reduced as the market diversifies.

Today's decision marks a major change in the UK's approach that will substantially improve the security and resilience of our critical telecoms networks. It will see the government roll out the most stringent set of controls ever – including new standards with tough underpinning legislation to raise the security and quality of the entire 5G and gigabit-capable networks.

Digital Secretary Baroness Morgan said:

> We want world-class connectivity as soon as possible but this must not be at the expense of our national security. High risk vendors never have been and never will be in our most sensitive networks.
>
> The government has reviewed the supply chain for telecoms networks and concluded today it is necessary to have tight restrictions on the presence of high risk vendors.
>
> This is a UK-specific solution for UK-specific reasons and the decision deals with the challenges we face right now.
>
> It not only paves the way for secure and resilient networks, with our sovereignty over data protected, but it also builds on our strategy to develop a diversity of suppliers.

> We can now move forward and seize the huge opportunities of 21st century technology.

Ciaran Martin, the Chief Executive of the National Cyber Security Centre, said:

> This package will ensure that the UK has a very strong, practical and technically sound framework for digital security in the years ahead.
>
> The National Cyber Security Centre has issued advice to telecoms network operators to help with the industry rollout of 5G and full fibre networks in line with the government's objectives.
>
> High risk vendors have never been – and never will be – in our most sensitive networks.
>
> Taken together these measures add up to a very strong framework for digital security.

Further background

The decision today concludes the Telecoms Supply Chain Review, first published in July 2019. The review was a comprehensive, evidence-based review, designed to ensure the security and resilience of the UK's networks.

It recommended new Telecoms Security Requirements (TSR) to provide clarity to the telecoms industry on what is expected in terms of network security.

The TSRs will raise the height of the security bar by setting out to telecoms operators – overseen by Ofcom and the government – the way to design and manage their networks to meet tough new standards.

Another area covered by the Review was how to treat those vendors which pose greater security and resilience risks to UK telecoms.

The Review also highlighted the need for the UK to improve the diversity in the supply of equipment to telecoms networks.

Today the government has announced the final conclusions of the Telecoms Supply Chain Review in relation to high risk vendors. The government, through the National Security Council, asked the NCSC to consider issuing guidance to UK Telecoms operators in relation to high risk vendors. That guidance has been published alongside the final conclusions of the Review.

Notes to editors

Read Baroness Morgan's Written Ministerial Statement to the House of Lords on UK Telecommunications

The NCSC has published a number of documents. These are:

DCMS press office can be contacted on 020 7211 2210.

Defra advice for imports during the transition period

As part of preparations for exiting the EU, Defra are issuing and collating guidance to ensure that businesses are aware of forthcoming changes and ready for Brexit.

There are no inmediate changes coming into effect on the 31 January, but Defra is making stakeholders aware about the changes that the EU are making to the pre-notification system.

More information is available

Published 28 January 2020

Assisted departure from Wuhan

Assisted departure from Wuhan

Due to the increasing travel restrictions and difficulty accessing medical assistance we are working to make an option available for British nationals to leave Hubei Province. This may happen quickly and with short notice.

If you are a British national in Hubei Province, please call our 24/7 number +86 (0) 10 8529 6600 or (+44) (0)207 008 1500 to register your desire to leave before 29th Jan 11am. Once arrangements are confirmed we will then contact you to confirm arrangements.

Read More: Travel advice in China

Published 28 January 2020