Tougher telecoms security rules to defend UK from cyber attacks

- New regulations and code proposed to raise telecoms security standards
- Will set out what telecoms providers must do to protect their networks and services
- Public consultation launched today on the proposals

Mobile and broadband networks will be better protected from cyber attacks under stronger security rules for telecoms companies proposed by the government.

The Telecommunications (Security) Act became law in November last year and puts much stronger legal duties on public telecoms providers to defend their networks from cyber threats which could cause network failure or the theft of sensitive data.

The government has today launched a public consultation on draft regulations, which outline the specific measures telecoms providers would need to take to fulfil their legal duties under the Act, and a draft code of practice on how providers can comply with the regulations.

The proposed measures and guidance, developed with the National Cyber Security Centre, aim to embed good security practices in providers' long term investment decisions and the day-to-day running of their networks and services.

Under the draft regulations telecoms providers will be legally required to:

- protect data stored by their networks and services, and secure the critical functions which allow them to be operated and managed;
- protect tools which monitor and analyse their networks and services against access from hostile state actors;
- monitor public networks to identify potentially dangerous activity and have a deep understanding of their security risks, reporting regularly to internal boards; and
- take account of supply chain risks, and understand and control who has the ability to access and make changes to the operation of their networks and services.

Digital Infrastructure Minister Julia Lopez said:

> Broadband and mobile networks are crucial to life in Britain and that makes them a prime target for cyber criminals.
>
> Our proposals will embed the highest security standards in our telecoms industry with heavy fines for any companies failing in their duties.

The consultation seeks views on plans to place telecoms providers into three ‘tiers’ via a new code of practice according to size and importance to UK connectivity. This will ensure steps to be taken under the code are applied proportionately and do not put an undue burden on smaller companies.

Currently, telecoms providers are responsible by law for setting their own security standards in their networks. But the Telecoms Supply Chain Review carried out by the government 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 created the Telecommunications (Security) Act to strengthen the overarching legal duties on providers of UK public telecoms networks and services as a way of incentivising better security practices.

Companies which fail to comply could face fines of up to ten per cent of turnover or, in the case of a continuing contravention, £100,000 per day. Ofcom will monitor and assess the security of telecoms providers.

NCSC Technical Director Dr Ian Levy said:

> Modern telecoms networks are no longer just critical national infrastructure, they are central to our lives and our economy.
>
> As our dependence on them grows, we need confidence in their security and reliability which is why I welcome these proposed regulations to fundamentally change the baseline of telecoms security.
>
> The NCSC has worked closely with DCMS and industry to propose and advise on the most effective measures that telecoms operators can take to ensure the resilience of UK broadband and mobile networks, now and into the future.

ENDS

Notes to editors

As part of the consultation, the government is particularly interested in feedback on:

- the specific measures set out in the draft regulations and draft code of practice;
- the proposed tiering system set out in the draft code of practice, which is intended to ensure it is implemented appropriately and proportionately;
- the proposed timescales to phase-in new measures in the draft code of practice; and
- the ways in which the draft code of practice and the draft regulations account for older, legacy equipment that is due to be phased out.

The consultation on the draft code of practice meets the requirement under section 105F in the Communications Act 2003 (as amended by the Telecommunications (Security) Act 2021) to consult with affected parties on the draft code of practice. The Government has chosen to consult on the draft regulations at the same time. This does not necessarily mean that future decisions to make, or vary, the regulations will be subject to similar consultation.

The Government will consider responses to the consultation to inform final policy decisions on the regulations and code of practice. The final regulations and the final code of practice will be laid in Parliament, as required by the Communications Act 2003 (as amended by the Telecommunications (Security) Act 2021).

The consultation will close on 10 May. The new regulations and code of practice are expected to come into force later this year.