Tough new rules confirmed to protect UK telecoms networks against cyber attacks

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

The Telecommunications (Security) Act, which became law in November, gives the government powers to boost the security standards of the UK's mobile and broadband networks, including the electronic equipment and software at phone mast sites and in telephone exchanges which handle internet traffic and telephone calls.

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

The new regulations and code of practice, developed with the National Cyber Security Centre and Ofcom, set out specific actions for UK public telecoms providers to fulfil their legal duties in the Act. They will improve the UK's cyber resilience by embedding good security practices in providers' long term investment decisions and the day-to-day running of their networks and services.

The substance of the final regulations has been confirmed by the government following a response to a public consultation on them published today. The regulations are to make sure providers:

- protect data processed by their networks and services, and secure the critical functions which allow them to be operated and managed
- protect software and equipment which monitor and analyse their networks and services
- have a deep understanding of their security risks and the ability to identify when anomalous activity is taking place with regular reporting to internal boards
- 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 to enhance security

Digital Infrastructure Minister Matt Warman said:

> We know how damaging cyber attacks on critical infrastructure can be, and our broadband and mobile networks are central to our way of life.
>
> We are ramping up protections for these vital networks by

> introducing one of the world’s toughest telecoms security regimes which secure our communications against current and future threats.

NCSC Technical Director Dr Ian Levy said:

> We increasingly rely on our telecoms networks for our daily lives, our economy and the essential services we all use.
>
> These new regulations will ensure that the security and resilience of those networks, and the equipment that underpins them, is appropriate for the future.

The regulations will be laid as secondary legislation in Parliament shortly, alongside a draft code of practice providing guidance on how providers can comply with them.

Ofcom will oversee, monitor and enforce the new legal duties 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.

From October, providers will be subject to the new rules and Ofcom will be able to use its new powers to ensure providers are taking appropriate and proportionate measures to meet their security duties and follow the guidance within the code of practice. This includes:

- identifying and assessing the risk to any ‘edge’ equipment that is directly exposed to potential attackers. This includes radio masts and internet equipment supplied to customers such as Wi-Fi routers and modems which act as entry points to the network
- keeping tight control of who can make network-wide changes
- protecting against certain malicious signalling coming into the network which could cause outages;
- having a good understanding of risks facing their networks
- making sure business processes are supporting security (e.g. proper board accountability)

Providers will be expected to have achieved these outcomes by March 2024. The code of practice will set out further timeframes for completion of other measures. The code will be updated periodically to ensure it keeps pace with any evolving cyber threats.

ENDS

Notes to editors

The government received responses to the consultation from public telecoms providers, suppliers and trade bodies. The government’s response sets out the ways in which those responses have been considered and reflected in the final

Regulations and draft Code of Practice.

Technical changes following the consultation include:

- clarification to ensure security measures are targeted at the parts of networks most in need of protection, like new software tools that power 5G networks
- inclusion of further guidance on national resilience, security patching and legacy network protections, to help providers understand actions that need to be taken

The Electronic Communications (Security Measures) Regulations will be laid in Parliament through a statutory instrument under the negative procedure.

The draft code of practice will be laid in Parliament under the requirement in section 105F of the Communications Act 2003 (as amended by the Telecommunications (Security) Act 2021). It will remain in draft for Parliamentary scrutiny for forty sitting days, after which the code of practice will be issued and published.