Joint statement from Ofcom and the National Cyber Security Centre

This is a public statement from Ofcom and the National Cyber Security Centre (NCSC) on how they will work together under the new Telecommunications (Security) Bill, currently in passage. It is intended to provide clarity for Parliament and industry.

The NCSC is the UK's technical authority on cyber security and advises the Secretary of State on national security matters relating to telecoms. Ofcom is the UK's communications regulator.

Ofcom has maintained a close and effective working relationship with NCSC since the latter's inception in 2016, with the NCSC providing expert technical advice on cyber security where relevant, to assist Ofcom in the exercise of its functions. This relationship will become even more important as Ofcom takes on new regulatory responsibilities for telecoms security under the Telecommunications (Security) Bill (the Bill).

As the UK's communications regulator, Ofcom is already responsible for enforcing the telecoms security provisions in sections 105A-D of the Communications Act 2003. This regulatory role will be expanded under the Telecommunications (Security) Bill, which introduces a new telecoms security framework, replacing sections 105A-D. Under the new framework, which is established by clause 1 to 14 of the Bill, Ofcom will monitor, assess and enforce industry compliance with the new telecoms security framework. In relation to high risk vendors Ofcom will have a more limited role, restricted to collecting information and reporting it to the Secretary of State when instructed to do so through monitoring directions under clause 105Z12 of the Bill.

Both Ofcom and the NCSC will continue to work together in a collaborative, open and transparent manner. Some key principles underpinning the relationship include:

- **The NCSC will provide expert technical cyber security advice to Ofcom to support its monitoring, assessment and enforcement of the new telecoms security framework.** The new telecoms security framework in the Bill was developed in collaboration with the NCSC, drawing on its technical expertise in cyber security matters relating to the telecoms sector. It is therefore likely that Ofcom will, where appropriate, require the NCSC's advice on certain technical matters relevant to the framework, including the measures set out in any Code of Practice issued by the Secretary of State under the Bill. The NCSC will act as an independent source of technical expertise only and will have no formal role in Ofcom's regulatory procedures. The need for technical advice from NCSC will decrease over time as Ofcom continues to expand its own technical expertise and resources.
- **Ofcom and the NCSC will exchange information where necessary and permitted by law**. The new statutory framework will require providers to share a greater volume of information related to telecoms security with Ofcom. Where appropriate and to the extent permitted by law this information will be shared with NCSC. Similarly, where appropriate and relevant to the exercise of Ofcom's functions, the NCSC will share intelligence with Ofcom about specific threats that are likely to affect organisations regulated by Ofcom. Information will not be shared if it is either commercially confidential or sensitive, unless the NCSC has received consent from the affected organisation to share such information.

- **The NCSC will provide incident management support during serious cyber security incidents to telecoms operators and to Ofcom as necessary.** This is consistent with the NCSC's responsibilities as the national cyber security technical lead. Importantly, the NCSC will not share incident-specific information with Ofcom unless it has the consent of the affected organisation. Where an organisation reports an incident to Ofcom, it will encourage the organisation to notify the NCSC and may elect to notify the NCSC itself where permitted to do so by law.