EXPLANATORY MEMORANDUM TO

THE REVISED TELECOMMUNICATIONS SECURITY CODE OF PRACTICE

1. Introduction

1.1 This Explanatory Memorandum has been prepared by the Department for Science, Innovation and Technology and is laid before Parliament by Command of His Majesty.

2. Declaration

2.1 Baroness Lloyd of Effra, Parliamentary Under-Secretary of State for Digital Economy at the Department for Science, Innovation and Technology, confirms that this Explanatory Memorandum meets the required standard.

2.2 David Haynes, Deputy Director for Telecoms Security and Resilience, at the Department for Science, Innovation and Technology, confirms that this Explanatory Memorandum meets the required standard.

3. Contact

3.1 Thomas Baker at the Department for Science, Innovation and Technology (DSIT) can be contacted by email at the following address with any queries regarding the instrument: telecomssecurityresilience@dsit.gov.uk. Alternatively, the department can be contacted by telephone: 07922 578186.

Part One: Explanation, and context, of the Instrument

4. Overview of the Instrument

What does the Revised Code do?

4.1 The Telecommunications (Security) Act 2021 amended the Communications Act 2003 ('the Act') to strengthen the security and resilience of public telecoms networks and services. Using powers in the Act, in 2022 the Government made the Electronic Communications (Security Measures) Regulations 2022 (S.I. 2022/933) ('the Regulations') and issued the Telecommunications Security Code of Practice ('the 2022 Code').

4.2 The Explanatory Memorandum relates to a revised version of this Code (the Revised Code). This Revised Code contains revisions to guidance on key telecoms network security concepts and technical measures to assist public telecoms providers in complying with duties in the Act and requirements in the Regulations.

4.3 This Revised Code provides detailed guidance to Tier 1[1] and Tier 2[2] public telecoms providers (as defined in paragraph 0.12 of the 2022 Code, and retained in paragraph 0.14 of the Revised Code) on the Government's preferred approach to demonstrating compliance with the duties in the Act and the requirements in the Regulations.

[1] Public telecoms providers with relevant turnover in the relevant period of £1bn or more.
[2] Public telecoms providers with relevant turnover in the relevant period of more than or equal to £50m but less than £1bn.

Where does the Revised Code extend to, and apply?

4.4 The extent of this instrument (that is, the jurisdiction(s) which the instrument forms part of the law of) is England and Wales, Northern Ireland, and Scotland.

4.5 The territorial application of this instrument (that is, where the instrument produces a practical effect) is England and Wales, Northern Ireland, and Scotland.

5. Policy Context

What is being done and why?

5.1 Following security advice provided by the UK's technical authority on cyber security, the National Cyber Security Centre (NCSC), the Government intends to issue the Revised Code to ensure that the technical guidance provided to public telecoms providers adequately reflects emerging threats and evolving technologies, and responds to requests from industry for additional technical guidance.

What was the previous policy, how is this different?

5.2 The Revised Code retains the original detailed technical guidance for large and medium sized public telecoms providers but, to help them meet their legal obligations under the Act and the regulations, it also contains new guidance on specific key concepts and technical measures.

5.3 This new guidance is intended to: reflect evolving technology, the use of which has increased since the 2022 Code was issued (for example, eSIMs); reflect emerging security threats, particularly hostile-state-linked cyber-attacks; provide further clarity in response to public telecoms providers' working experience with the 2022 Code; and reemphasise the need for public telecoms providers to take a holistic approach to the security guidance set out within the Revised Code.

5.4 Specific revisions to the Revised Code include but are not limited to:

5.5 New guidance on network automation which aligns the Revised Code with existing guidance from the NCSC, including on secure principles for machine learning[3].

- New guidance on signalling (used to control how connections are set up, maintained, routed and cleared), to address feedback from industry and the continued targeting of the signalling plane by cyber threat actors.
- New guidance, and amendments to existing guidance, on privileged access workstations (devices used to access and make changes to the most security critical parts of the network) to align the Revised Code with European Telecommunications Standards Institute (ETSI) standards[4].
- New guidance on Application Programming Interfaces (rules or protocols that enable software applications to communicate with each other), which have become more routinely used and linked to significant data losses.
- New guidance on patching and updates, to mitigate threats posed by non-persistent malware.

[3] https://www.ncsc.gov.uk/collection/machine-learning-principles
[4] https://www.etsi.org/deliver/etsi_ts/103900_103999/10399401/01.01.01_60/ts_10399401v010101p.pdf

6. Legislative and Legal Context

How has the law changed?

6.1 The law has not changed. The Revised Code provides technical guidance to public telecoms providers on the Government's preferred approach to demonstrating compliance with the duties in the Act and the requirements in the Regulations.

Why was this approach taken to change the law?

6.2 This is the only possible approach to make the necessary changes, pursuant to ss. 105E(b) and 105F of the Act.

7. Consultation

Summary of consultation outcome and methodology

7.1 The Government, in the 2022 Code, established that "where changes to the Code of Practice are proposed, the government will consult affected public telecoms providers, Ofcom, and any other relevant parties".

7.2 Public telecoms providers and Ofcom, as well as the wider public, were consulted on a set of proposed revisions to the 2022 Code through an eight-week public consultation held between 28th August and 22nd October 2025. In addition, a survey was circulated to the UK's large and medium public telecoms providers between 25th November and 28th January 2026 (nine weeks) seeking feedback on potential cost impacts of the changes.

7.3 In total, 30 responses were received to the consultation, and 7 responses were received to the additional cost survey. Respondents broadly supported the overall intent of the proposed revisions, but raised concerns about potential costs, implementation timelines, and the technical feasibility of some proposals.

7.4 The Government carefully reviewed all consultation feedback and cost survey returns. In response, the Government made amendments to the proposed revisions that were consulted upon where appropriate. The Government response to the consultation has been published on GOV.UK[5]. It sets out how the views of respondents were considered and where amendments were made to the draft of the Revised Code that was consulted on.

8. Applicable Guidance

8.1 The Revised Code is itself guidance and is aligned to guidance on various topics issued by various bodies such as NCSC and ETSI. No guidance is planned to be produced to specifically accompany the Revised Code.

Part Two: Impact and the Better Regulation Framework

9. Impact Assessment

9.1 A full Regulatory Impact Assessment has not been prepared for this instrument. The instrument revises the 2022 Code and provides guidance on how public telecommunications providers may demonstrate compliance with existing statutory security duties under the Act, as amended by the Telecommunications (Security) Act 2021, and the Regulations. The instrument does not introduce new statutory duties or

[5] https://www.gov.uk/government/consultations/proposals-to-update-the-telecommunications-security-code-of-practice-2022

regulatory requirements and therefore does not constitute a regulatory provision under the Better Regulation Framework.

Impact on businesses, charities and voluntary bodies

9.2 The impact on in-scope telecommunications providers (Tier 1 and Tier 2 telecommunications providers with relevant turnover above £50 million) is expected to result in a low overall financial impact. The main impacts are expected to arise as a result of familiarisation with the Revised Code, and from the implementation of further technical and organisational processes to address evolving security threats and technological developments.

9.3 Based on analysis undertaken by DSIT, the familiarisation costs associated with the Revised Code are expected to be negligible. Where providers implement changes in line with the revised guidance, indicative estimates suggest potential one-off implementation costs in the order of £1.9 million to £3.2 million per provider, with ongoing annual costs of approximately £285,000 to £445,000 per provider. These estimates are indicative and subject to variation depending on provider size, network architecture, and existing security maturity. When considered in the context of the scale and revenues of the UK telecommunications sector, these costs are minor.

9.4 The main benefits of the Revised Code arise from improved clarity and consistency in how security duties should be complied with in practice, supporting enhanced resilience of UK telecommunications networks that underpin critical national infrastructure, public services and economic activity. While these benefits are not readily quantifiable, they relate to a reduced likelihood and potential impact of security incidents, reduced risk of service disruption, and greater confidence in the security of digital infrastructure.

9.5 There is no, or no significant, impact on other business, charities or voluntary bodies because the Revised Code only applies to Tier 1 and Tier 2 public telecoms providers.

9.6 The Revised Code does not impact small or micro businesses.

9.7 There is no, or no significant, impact on the public sector, including on Ofcom, because the Revised Code only applies to Tier 1 and Tier 2 public telecoms providers.

10. Monitoring and review

What is the approach to monitoring and reviewing the Revised Code?

10.1 The approach to monitoring, as outlined in paragraph 0.32 of the Revised Code, is to "review and update the Code of Practice periodically as new threats emerge and technologies evolve".

10.2 As the Revised Code is technical guidance, and not legislation, no statutory review clause is required.

Part Three: Statements and Matters of Particular Interest to Parliament

11. Matters of special interest to Parliament

11.1 None.

12. European Convention on Human Rights

12.1 As the instrument is subject to the negative procedure, and does not amend primary legislation, no statement is required.

13. The Relevant European Union Acts

13.1 This instrument is not made under the European Union (Withdrawal) Act 2018, the European Union (Future Relationship) Act 2020 or the Retained EU Law (Revocation and Reform) Act 2023 ("relevant European Union Acts").