EXPLANATORY MEMORANDUM TO

THE ELECTRONIC COMMUNICATIONS (SECURITY MEASURES) REGULATIONS 2022

2022 No. 933

1. Introduction

1.1 This explanatory memorandum has been prepared by the Department for Digital, Culture, Media and Sport and is laid before Parliament by Command of Her Majesty.

1.2 This memorandum contains information for the Joint Committee on Statutory Instruments.

2. Purpose of the instrument

2.1 To establish specific security measures that providers of public electronic communications networks or public electronic communications services must take to fulfil their duties under sections 105B and 105D of the Communications Act 2003 (hereafter "the Act").

2.2 Section 105B of the Act enables the Secretary of State to make regulations that require providers of public electronic communications networks or services ("public telecommunications providers") to take specific measures that are appropriate and proportionate to identify and reduce the risk of security compromises occurring and prepare for security compromises (as defined in 105A(2) of the Act).

2.3 Section 105D of the Act enables the Secretary of State to make regulations that require public telecommunications providers to take specific measures in response to security compromises. These measures may be specified if the Secretary of State considers that taking that measure, or a measure of that description, would be appropriate and proportionate for the purpose of preventing adverse effects (on the network or service or otherwise) arising from a security compromise of the specified description. They may also be specified if the Secretary of State considers that taking that measure, or a measure of that description, would be appropriate and proportionate for the purpose of remedying or mitigating an adverse effect of the specified description.

3. Matters of special interest to Parliament

Matters of special interest to the Joint Committee on Statutory Instruments

3.1 None.

4. Extent and Territorial Application

4.1 The territorial extent of this instrument is the United Kingdom.

4.2 The territorial application of this instrument is the United Kingdom.

5. European Convention on Human Rights

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

6. Legislative Context

6.1 This instrument exercises powers inserted into the Act by the Telecommunications (Security) Act 2021. The instrument forms part of a new telecoms security framework created by the Telecommunications (Security) Act 2021. This consists of overarching security duties on public telecommunications providers to identify, reduce and prepare for security compromises and to remedy or mitigate their adverse effects. It also provides new powers for the Government to make regulations (contained in this instrument) setting out specific security measures to be taken by providers under section 105B and 105D of the Act. Finally the framework includes new powers to issue codes of practice containing technical guidance on how public telecommunications providers can meet their legal obligations.

6.2 The powers to make the regulations contained in this instrument were debated in both Houses during passage of the Telecommunications (Security) Act in the second session.

7. Policy background

What is being done and why?

7.1 The UK's future prosperity rests on the security and resilience of the public electronic communications networks and services that connect us. Such networks and services are fundamental to supporting our modern quality of life. Public telecommunications providers deliver the connectivity that enables people, communities and businesses to carry out their daily activities across the UK. Disruption to those activities would undermine the normal functioning of our society and public order. Yet as technologies evolve, new threats to those networks and services are emerging.

7.2 In 2011 there were security duties inserted into the Act (sections 105A-D). Under those provisions, providers were required to take technical and organisational measures appropriately to manage risks to the security of their networks and services. However, the UK Telecoms Supply Chain Review, conducted between 2018 and 2019, found that industry security practices were inadequate to address growing risks. These practices were in turn driven by a lack of incentives to manage risk, including the inability of the regulatory framework to drive improvements in cyber security.

7.3 The Telecommunications (Security) Act 2021 established a new telecoms security framework to enable the Government, Ofcom and industry to address the most pressing risks to networks and services. This new framework replaces the former sections 105A-D. Security risks to networks and services can never be completely prevented, but the measures in this instrument will ensure public telecoms providers in the UK take the right steps to protect their public networks and services against security threats.

7.4 The measures contained in this instrument have been informed by extensive and detailed analysis of the security of the telecoms sector carried out by the National Cyber Security Centre, as the UK's national technical authority for cyber security. The analysis was developed around priority threats which have been identified through thorough testing and the real-world experiences of public telecommunications providers and a summary was published by the NCSC in January 2020.[1] A draft of this instrument, informed by the NCSC's analysis, was put to public consultation on 1 March 2022 and that consultation closed on 10

[1] *Summary of the NCSC's security analysis for the UK telecoms sector*, https://www.ncsc.gov.uk/files/Summary%20of%20the%20NCSCs%20security%20analysis%20for%20the%20UK%20telecoms%20sector.pdf

May 2022. The responses to that consultation (detailed in section 10 below) informed the regulations contained in this instrument.

7.5 This instrument contains sixteen regulations.

7.6 Regulation 1 concerns the citation, territorial extent and commencement date of the regulations, which is 1 October 2022.

7.7 Regulation 2 (Interpretation) sets out the specific definitions used throughout the instrument.

7.8 Regulation 3 (Network architecture) requires public electronic communication network providers ("network providers") to take appropriate and proportionate measures to securely design, construct and (where relevant) redesign, develop, and maintain their public network. To achieve this, the measures focus on ensuring network providers understand the risks of security compromises to network architecture, record those risks, and act to reduce them. This includes securely maintaining networks serving the UK by ensuring that network providers can identify security risks and, where necessary, operate the network without reliance on persons, equipment or stored data located outside the UK.

7.9 Regulation 4 (Protection of data and network functions) requires network providers and providers of public electronic communication services ("service providers") to take appropriate and proportionate technical means to protect the data stored in relation to the operation of networks and services, and secure the functions that allow networks and services to be operated and managed effectively. These functions include the software, devices and equipment that manage and run networks and services. The measures will make sure network and service providers protect against malicious incoming signals, secure the workstations used to make changes to their public networks, and reduce the risk of security compromise relating to customers' SIM cards.

7.10 Regulation 5 (Protection of certain tools enabling monitoring and analysis) requires network or service providers to take measures to protect monitoring and analysis tools by ensuring that network and service providers account for location-related risks. This includes ensuring that monitoring and analysis tools are not located in, or accessible from, countries listed in the Schedule to the regulations. These countries are China, Iran, North Korea and Russia. Where providers host capabilities in other non-UK locations, they must take measures to identify and reduce the risks of security compromise occurring as a result of monitoring and analysis tools being stored on equipment in those locations.

7.11 Regulation 6 (Monitoring and analysis) requires network or service providers to take appropriate and proportionate measures to maintain oversight of access to networks and services in order to reduce the risk of security compromises. This includes securely retaining logs relating to security critical function access for at least 13 months, as well as having systems to ensure providers are alerted to and can address unauthorised changes to the most sensitive parts of the network or service.

7.12 Regulation 7 (Supply chain) requires network or service providers to take appropriate and proportionate measures with their third party suppliers to help to identify and reduce risks of security compromise. To achieve this, network or service providers will need to take appropriate and proportionate measures to ensure contractual arrangements with their third party suppliers which, among other things, require those suppliers to take appropriate measures to identify, disclose and reduce risks of security compromises arising from the relationship. Network or service providers are also required to have written contingency plans that set out what steps will be taken in the event that supply from a third party is interrupted. Where a third party supplier given access to sensitive data or equipment is also a network

provider, that provider must take the equivalent steps as the primary provider it is supplying in relation to that data or equipment.

7.13 Regulation 8 (Prevention of unauthorised access or interference) requires network or service providers to take appropriate and proportionate measures to reduce the risk of security compromises occurring as a result of unauthorised access to their public networks or services. It ensures providers understand and control who has the ability to access and make changes to the operation of their public networks and services to avoid security compromises. Providers will need to follow requirements that include applying best practice such as multi-factor authentication and password protections for users who have the ability to make changes to security critical functions. Alongside technical solutions, network and service providers must give approval for staff permissions and be responsible for people's access to administrative accounts, including access by third parties.

7.14 Regulation 9 (Preparing for remediation and recovery) requires network or service providers to take appropriate and proportionate measures to prepare to mitigate the adverse impacts of security compromises and be able to successfully recover in the event of such a compromise. This includes holding and updating copies of information needed to rebuild the public network or service in the event of a security compromise. It also makes sure providers have processes in place to appropriately respond to, mitigate and recover from security compromises.

7.15 Regulation 10 (Governance) requires network or service providers to take appropriate and proportionate measures to ensure that those given responsibility for securing public telecoms networks or services are managed appropriately and are adopting appropriate security policies. Network or service providers will need to assign board-level responsibility (or equivalent) for oversight of new governance processes and effective management of persons responsible for taking security measures within the organisation. The regulation also sets out how to put an organisational framework in place to manage security incidents from a business process perspective.

7.16 Regulation 11 (Reviews) requires network or service providers to regularly review the security of their networks and services to identify and address security risks. These must be carried out at least once every 12 months. Written assessments must include an assessment of the overall risks of security compromises occurring in the following 12 months.

7.17 Regulation 12 (Patches and updates) requires network or service providers to make the effective use of security patches and upgrades to protect physical and virtual networks and services against attacks. This includes taking appropriate and proportionate steps to apply patches provided by software or equipment providers within 14 days, unless there is a particular circumstance requiring a longer period. When taking longer than 14 days, providers must have regard to the severity of risk that the patch or mitigation measures addresses, and record the reasons for this extension.

7.18 Regulation 13 (Competency) requires network or service providers to take appropriate and proportionate measures to ensure that those responsible for understanding and managing security risks in a provider's network or service are suitably skilled and experienced. Network or service providers will need to follow the requirements that set out the ways in which responsible persons should be competent in fulfilling their security duties under the Act and should be given resources to enable them to do so.

7.19 Regulation 14 (Testing) requires network or service providers to carry out, at appropriate intervals, tests to assess the risks of security compromises to their public

networks and services. Such tests must simulate the actions of an attacker and be carried out without prior warning being given to staff.

7.20 Regulation 15 (Assistance) requires network or service providers to take appropriate and proportionate steps to share information and provision of assistance between public telecom providers to remedy or mitigate the effects of security compromises. Any information shared is only for the purposes of helping that provider identify and reduce the risks of a security compromise occurring. Any such information sharing and assistance remains subject to competition laws.

7.21 Regulation 16 (Exemption for micro-entities) prevents the regulations contained in the instrument from applying to businesses that are classed as micro-entities, as defined under the Companies Act 2006.

8. European Union Withdrawal and Future Relationship

8.1 This instrument does not relate to withdrawal from the European Union / trigger the statement requirements under the European Union (Withdrawal) Act.

9. Consolidation

9.1 This instrument is the first made under the amended sections 105B and 105D of the Act and does not consolidate existing law.

10. Consultation outcome

10.1 Whilst there is no statutory requirement to consult on this instrument, as it is the first of its kind and will impact on industry, a ten-week public consultation was held on the draft content of this instrument and an accompanying draft code of practice. This took place from 1 March 2022 to 10 May 2022. A consultation document was published on GOV.uk alongside the draft instrument and draft code, setting out the government's rationale for their contents. A copy of this consultation document was also deposited in House libraries.

10.2 Prior to the public consultation, the government held regular cross-stakeholder and bilateral engagement beginning in January 2020. This has included engagement on the detail of proposed approaches to securing networks and services, held with public telecoms providers, their suppliers, and representative trade bodies. The NCSC and Ofcom were also represented in this engagement. This process informed the draft documents released for public consultation.

10.3 The consultation sought views on four areas: the ways in which public networks and services should be secured; the approach to defining companies in scope of the new measures; the approach to expected implementation timetables; and the approach to securing older "legacy" networks and services due to be phased out.

10.4 The government conducted a full assessment of all responses to the public consultation, and amended the instrument and accompanying code of practice based on its assessment. In total 38 responses were received, with respondents largely welcoming the introduction of new regulations and guidance to improve the security of public telecoms networks and services. Concerns raised centred on the proposed timeframes for implementing new measures, the technical feasibility of some of the protections proposed for securing network architecture, and the ways in which telecoms providers would be expected to interact with their suppliers and one another. A government response to the consultation has also been

published that sets out how these views were considered and where these resulted in amendments to the documents that were consulted on.[2]

11. Guidance

11.1 This instrument is accompanied by a draft code of practice, which has been laid before Parliament to meet the statutory requirement in section 105F of the Act. The final code of practice will be issued and published following the passage of forty sitting days, unless either House resolves not to approve it.

11.2 The draft code of practice contains detailed technical guidance for certain public telecommunication providers, to help them fulfil their obligations in the Act and the regulations contained in this instrument. It sets out how providers may determine whether guidance is applicable, via a system of tiering with tier thresholds being determined by a provider's annual relevant turnover[3]. The draft code of practice sets out three tiers, so that greater responsibilities are placed on those for whom a compromise is likely to have the most damaging security, economic or social effects. The draft code of practice also sets out indicative timeframes by which certain providers would be expected to have taken specific measures.

11.3 The effects of the code of practice are set out in section 105H of the Act. These indicate the status of the code of practice as guidance, that Ofcom must take the code of practice into account when carrying out its regulatory duties and functions, and that the code of practice may be considered in legal proceedings. Providers have a duty to explain any failure to act in accordance with a provision contained in the code of practice, if asked to do so by Ofcom, under section 105I of the Act.

12. Impact

12.1 The impact on business has been assessed at a best estimate cost of £4.1bn over a ten-year period. This cost was calculated using data returned by respondents to a survey issued by the Department. The survey was issued to public telecoms providers alongside the public consultation on the draft instrument and accompanying draft code of practice. The data returned indicated costs for the instrument as a whole and its individual subsections.

12.2 The benefits of the regulations contained in this instrument are linked to successful reduction and management of risks, and will be dependent on how threats to telecoms security may emerge. However, the cost of a single security compromise for a public telecoms provider can be up to £250m. Implementation of the regulations contained in this instrument will reduce the total cost of such compromises.

12.3 There is no, or no significant, impact on charities or voluntary bodies.

12.4 The impact on the public sector over a ten-year period is between £53m and £70m for costs to Ofcom under its new regulatory responsibilities; and between £0.9m and £1.4m for costs to the Department.

---

[2] https://www.gov.uk/government/consultations/proposal-for-new-telecoms-security-regulations-and-code-of-practice/outcome/proposals-for-new-telecoms-security-regulations-and-code-of-practice-government-response-to-public-consultation

[3] Relevant turnover is an existing metric used by Ofcom to determine the level of its charges levied on regulated companies. Detail is available at https://www.ofcom.org.uk/__data/assets/pdf_file/0017/80801/definition_of_relevant_acitvity_guidelines.pdf

12.5 A full Impact Assessment is submitted with this memorandum and published alongside this memorandum on the legislation.gov.uk website.

13. Regulating small business

13.1 The legislation applies to activities that are undertaken by small businesses. However the legislation does not apply to activities that are undertaken by micro-businesses.

13.2 To minimise the impact of the requirements on small businesses (employing up to 50 people), the approach taken is twofold. Firstly, the regulations set out in this instrument indicate where providers must take measures that are appropriate and proportionate to their businesses and the risk they seek to mitigate. Secondly, a system of tiering has been applied to the measures contained in the accompanying draft code of practice. This distinguishes between large and medium-sized providers, to whom the detailed guidance in the code of practice will apply, and smaller providers who may choose to adopt the guidance measures where these are relevant to their networks and services. Ofcom has indicated that it will apply different levels of oversight to these large, medium and small public telecoms providers, reflecting the relative importance of providers within each tier.

14. Monitoring & review

14.1 Section 14 of the Telecommunications (Security) Act 2021 requires the Secretary of State to carry out reviews of the impact and effectiveness of sections 1 to 13 of that Act. The provisions subject to review include those that inserted in the Act the powers under which the regulations are made. In view of this existing duty to review, it is not regarded as appropriate to make provision for review in these regulations.

14.2 The review will take place by October 2027 to ensure that the new telecoms security framework:

- has achieved its original objectives;
- has objectives that remain appropriate;
- is still required and remains the best option for achieving these objectives.[4]

14.3 The instrument therefore does not include a statutory review clause.

15. Contact

15.1 Daniel Tor at the Department for Digital, Culture, Media and Sport (Daniel.Tor@dcms.gov.uk) can be contacted with any queries regarding the instrument.

15.2 Kathryn Roe, Deputy Director for Telecoms Security and Resilience at the Department for Digital, Culture, Media and Sport can confirm that this Explanatory Memorandum meets the required standard.

15.3 Matt Warman, the Minister of State at the Department for Digital, Culture, Media and Sport can confirm that this Explanatory Memorandum meets the required standard.

[4] This includes consideration of whether the objectives could be achieved in another way which involves less onerous regulatory provision to reduce the burden on business and/or increase overall societal welfare.