EXPLANATORY MEMORANDUM TO

THE PRODUCT SECURITY AND TELECOMMUNICATIONS INFRASTRUCTURE (SECURITY REQUIREMENTS FOR RELEVANT CONNECTABLE PRODUCTS) REGULATIONS 2023

2023 No. 1007

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. Purpose of the instrument

2.1 This instrument exercises powers provided by Part 1 of the Product Security and Telecommunications Infrastructure (PSTI) Act 2022, and section 8C of the European Union (Withdrawal) Act 2018. Alongside the PSTI Act, this instrument delivers the Government's commitment in January 2020 to introduce a legislative regime preventing consumer connectable products from being sold to UK customers unless their manufacturers are compliant with fundamental security requirements. This instrument makes provision necessary for the regime established in the PSTI Act to come into effect, detailed further in section 6 of this memorandum.

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 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 The Viscount Camrose, Minister for AI and Intellectual Property, has made the following statement regarding Human Rights:

"In my view the provisions of the Product Security and Telecommunications Infrastructure (Security Requirements for Relevant Connectable Products) Regulations 2023 are compatible with the Convention rights."

6. Legislative Context

6.1 This instrument forms a part of the new consumer connectable product security regime created by Part 1 of the PSTI Act. It exercises powers in that Act, as well as the power in section 8C of the European Union (Withdrawal) Act 2018, to make provisions necessary for that regime to come into effect. This instrument includes the security requirements that manufacturers of UK consumer connectable products will need to comply with and conditions for deemed compliance with these requirements as an alternative to the relevant security requirement.

6.2 This instrument also contains descriptions of excepted products to which it is not currently appropriate for the regime to apply. Finally, there are provisions relating to the statement of compliance that must accompany a product, enabling businesses in the entire supply chain to prevent insecure products from being supplied to UK customers.

6.3 The powers in the PSTI Act under which this instrument is made, as well as the Government's intention for the provision to be made in this instrument, were debated in both Houses during the passage of the PSTI Act. During those debates, and in response to parliamentary questions during and subsequent to the passage of the Act, the Government repeatedly reiterated its commitment to bringing forward security requirements based on provisions 5.1-1, 5.1-2, 5.2-1, and 5.3-13 of the leading international standard for consumer internet of things (IoT) cyber security - ETSI EN 303 645 (henceforth referred to as "the EN"). Schedule 1 of this instrument sets out requirements that deliver on that commitment.

7. Policy background

What is being done and why?

7.1 The innovations that have enabled an increasingly diverse range of consumer products to connect to networks have unlocked a myriad of benefits for the consumers and businesses that use these products and for the businesses that manufacture them. However, the connectability that underpins the benefits offered by these products also exposes them and their users to unacceptable cyber security risks. Connectable products inherently represent additional attack vectors for hackers which, if compromised, can result in harms including loss of personal data, cyber fraud, and, as these devices are increasingly integrated into every aspect of our lives, even physical harm.

7.2 Additionally, where the user authentication mechanisms used on these products are inadequately secure, they can be compromised en masse, allowing malicious actors to leverage their collective computing power to launch significant attacks against individuals, businesses, critical national infrastructure, and nation states. In 2016, cyber criminals used hundreds of thousands of compromised connectable products to launch Distributed Denial of Service (DDOS) attacks that disrupted the services of major news and media organisations such as the BBC and Netflix, as well as leaving much of the internet inaccessible across the US east coast.

7.3 The Government wants to ensure that the UK is one of the most secure places in the world to live and do business online. Empowering consumers to harness the benefits offered by connectable products without exposing themselves, or others, to unacceptable cyber risk is fundamental in delivering that objective. It is for this reason that the Government committed in both the 2016 and 2022 National Cyber Security Strategies to ensure that essential security requirements relating to these products are met when they are sold to UK customers.

7.4 Whether it be product design considerations, or the processes operated to maintain security levels across a product's life cycle, the manufacturers of these products have the most agency to address the security risks associated with their products. The UK published a voluntary code of practice in 2018 to support manufacturers of consumer connectable products in implementing basic security measures, but the slow adoption of the guidelines it set out, with only 27% of manufacturers having a mechanism for

the reporting of security vulnerabilities in place as of 2022, necessitates further government intervention. Evidence also suggests that whilst consumers value and consider the security of a product when making purchasing decisions, they assume that products available for them to purchase will not expose them to avoidable risk. The information asymmetry between consumers and manufacturers regarding the security of connectable products is a market failure that prevents consumers from incentivising better security practices through market forces. The Government is addressing this market failure through the PSTI Act and this instrument.

7.5 The PSTI product security regime will therefore mandate that manufactures abide by three security requirements. These are based on three of the guidelines from the 2018 Code of Practice for Consumer IoT Security which in the opinion of the National Cyber Security Centre, will make the most fundamental difference to the security of consumer connectable products:

- Universal default passwords, and easily guessable default passwords, which, if compromised, can allow malicious actors to compromise devices at scale, affording them with significant computing power with which to launch subsequent attacks, will be banned.
- Manufacturers will be obligated to maintain an awareness of existing and emergent security issues relating to the security of their products by publishing contact information for the reporting of these issues.
- Evidence suggests that UK consumers consider and value security when making purchasing decisions, and to better incentivise manufacturers to take this into account, they will be required to be transparent about how long their products will be supported with security updates for.

7.6 This regime, including the initial security requirements it mandates, have both been subject to extensive consultation with industry, cyber security subject matter experts, third sector organisations, and international partners. The 2018 Code of Practice for Consumer IoT Security was developed in collaboration with an Expert Advisory Group including industry, academics, and consumer associations. Additionally, the Government conducted consultation exercises on the legislative proposals of this regime in 2019 and 2020 (detailed in section 10 of this Memorandum).

7.7 The Government confirmed its approach for regulating consumer connectable product security in an April 2021 call for views response. The 10 regulations in this instrument, in combination with Part 1 of the PSTI Act, give effect to the policy positions set out in that response.

7.8 Regulation 1 concerns the citation, territorial extent and commencement date of the regulations in the instrument. It provides that they come into force on 29 April 2024, which is the same day that Part 1 of the PSTI Act comes into force, as per regulation 3 of The Product Security and Telecommunications Infrastructure Act 2022 (Commencement No.2) Regulations 2023.

7.9 Regulation 2 provides definitions for key terms used in the remainder of this instrument, as well as indicating that references to sections in this instrument refer to sections of the PSTI Act unless otherwise stated.

7.10 Regulation 3 provides that the security requirements set out in Schedule 1 to this instrument apply to manufacturers of relevant connectable products. In doing so, it ensures that manufacturers subject to the duty in section 8 of the PSTI Act must comply with these requirements, and confirm that they have complied with these

requirements in the statement of compliance accompanying the product to discharge the duty in section 9(2) of the PSTI Act.

7.11 Schedule 1 honours the Government's commitment to mandate requirements based on the top three guidelines of the 2018 Code of Practice, and the associated provisions of the EN:

- The requirement in paragraph 1 proscribes the use of universal default passwords or easily guessable default passwords. It is based on provisions 5.1-1 and 5.1-2 of the EN.
- The requirement in paragraph 2 mandates the publication of information relating to how security issues can be reported to the manufacturer. It is based on provision 5.2-1 of the EN.
- The requirement in paragraph 3 mandates the publication of the period of time over which security updates will be provided for the product (the "defined support period"). It is based on provision 5.3-13 of the EN.

7.12 Schedule 1 also realises the intention, confirmed in the Government's 2021 call for views response, for the requirements in paragraph 2 and 3 to extend to appropriate software associated with the product's intended functionality, whether or not that software is installed or installable on the product. For example, this could include cloud services or companion applications.

7.13 Regulation 4 provides that, where the conditions in Schedule 2 are met, a manufacturer is to be treated as having complied with a particular security requirement. These conditions relate to compliance with equivalent provisions to each requirement in appropriate international standards taken from either the EN, or ISO IEC 29147.

7.14 Regulation 5 ensures that, where multiple persons in the supply chain of a product meet the definition of "manufacturer" in section 7 of the PSTI Act, each of those persons must individually comply with the security requirements, whether by complying with the requirements themselves in Schedule 1, or meeting the corresponding deemed compliance conditions in Schedule 2. This provision ensures that where a business purchases unlabelled connectable products ("white label products") and sells them under their name or trade mark, that business, as well as the original equipment manufacturer, will each have to comply with the security requirements.

7.15 Regulation 6 provides that the PSTI product security regime will not apply in relation to products described in Schedule 3 of this instrument. The justifications for the products described in Schedule 3 being excluded from this regime are summarised below.

7.16 Under the terms of the EU Withdrawal agreement, some EU law (listed in Annex 2 of the Windsor Framework) continues to apply in Northern Ireland following the UK's withdrawal from the EU. Some of these laws ensure that, where they have been complied with, certain products can continue to move freely between Northern Ireland and the European Union. Products covered by these provisions include pyrotechnic articles, lifts, personal watercraft, and autonomous vehicles.

7.17 Paragraph 1 of Schedule 3 uses the power provided by section 8C of the European Union (Withdrawal) Act 2018 to provide that the regime does not extend to these products where they are made available for supply in Northern Ireland. In doing so,

this regime upholds the UK's international commitments under the EU Withdrawal Agreement, whilst ensuring that the protections and benefits offered by this regime are available to consumers and businesses across the UK.

7.18 Electric vehicle smart charge points, medical devices, and smart meters (and their associated products) are excepted from this regime by paragraphs 2, 3, and 4 of Schedule 3 respectively. This ensures that the regime does not impose unnecessarily duplicative regulatory burdens on the supply chains of products that are already subject to UK cyber security regulation.

7.19 Paragraph 5 of Schedule 3 excepts conventional IT products, including personal computers and tablets computers (that lack cellular connectivity capabilities) from the scope of this regime. The security of conventional IT products is not currently subject to targeted regulation in the UK. However, responses to the 2020 call for views highlighted that the manufacturers of these products would face unique challenges in complying with this regime due to the complexities of their supply chains. As the threat landscape affecting these products also differs from those of consumer connectable products more broadly, the Government has committed to exploring these challenges further with industry before taking any steps to bring them into scope of this regime.

7.20 Regulation 7 provides that the information specified in Schedule 4 must be included in the statement of compliance accompanying a product for a manufacturer to discharge the duty in section 9(2) of the PSTI Act. This information aligns to that required in the equivalent declaration of conformity under product safety legislation, and includes the name and address of each manufacturer of the product, and a declaration that they have complied with their security requirements.

7.21 To ensure that the enforcement authority is able to access important information relating to a product when investigating instances of possible non-compliance, regulations 8 and 9 require manufacturers and importers of relevant connectable products respectively to retain copies of a product's statement of compliance for the longer of 10 years, or the product's defined support period set out in that statement of compliance.

7.22 Regulation 10 is a statutory review clause in line with the requirements of the requirements of the Small Business, Enterprise and Employment Act 2015. Further details of the Government's intentions for reviewing the effectiveness of this regime are set out in section 14 of this instrument.

Explanations

What did any law do before the changes to be made by this instrument?

7.23 Article 5(4) of the Windsor Framework provides that certain European Union laws (those listed in Annex 2) continue to apply to and in the United Kingdom in respect of Northern Ireland. These include Directives and Regulations intended to harmonise the regulation of products across the European Union. Whilst the approach taken to ensure the free movement of goods between individual regulatory regimes, some of the EU laws applicable in Northern Ireland include provision that precludes Member States and the United Kingdom in respect of Northern Ireland from restricting the making available of certain products, provided the laws containing those provisions have been complied with. Examples of such provision include those on pyrotechnic articles, lifts, personal watercraft, and autonomous vehicles.

Why is it being changed?

7.24 The Regulations in this instrument do not amend any existing law, whether retained EU law, or otherwise.

What will it now do?

7.25 The power in section 8C of the European Union (Withdrawal) Act 2018 has been used to except products from this regime subject to EU legislation that prohibits the imposition of further regulatory restrictions relating to their supply (see paragraphs 7.16 and 7.17 of this memorandum for further details). These products will only be excepted from the regime where they are made available for supply in Northern Ireland.

8. European Union Withdrawal and Future Relationship

8.1 This instrument is not being made to address a deficiency in retained EU law but relates to the withdrawal of the United Kingdom from the European Union because the provision in paragraph 1 of Schedule 3 is for the purpose of dealing with matters related to the Windsor Framework, and is therefore made using the power in section 8C of the European Union (Withdrawal) Act 2018. The Minister has made any relevant statements in Part 2 of the Annex to this Explanatory Memorandum.

9. Consolidation

9.1 No consolidation is required.

10. Consultation outcome

10.1 The product security regime established by this instrument alongside Part 1 of the PSTI Act were both subject to extensive public consultation, supplemented by workshops with industry representatives and cyber security experts, as well as direct engagement with industry, international partners, academia, cyber security subject matter experts, and civil society organisations. In May 2019, the Government launched a consultation on legislative proposals for the cyber security of consumer connectable products. Responses to the consultation demonstrated widespread support for the introduction of a mandatory cyber security baseline aligned with priority security requirements as outlined in the Code of Practice - the requirements specified in this instrument. Responses to the Government's July 2020 Call for Views on proposals included in this instrument indicated further support for both its introduction, and the security requirements that will be mandated through this instrument.

10.2 The devolved administrations have been engaged during the development of this instrument and the PSTI Act.

11. Guidance

11.1 Non-statutory Guidance to support industry compliance with the requirements in this instrument, and the broader product security regime, will be provided by the appointed enforcement authority for this regime - the Office for Product Safety and Standards. This guidance will be made available on the gov.uk website before the regime enters into force.

12. Impact

12.1 The impact on business, charities or voluntary bodies is £187.3m over the 10 year appraisal period in the Department's central estimate. This cost was calculated using the best available evidence, including bespoke commissioned studies, and multiple industry consultation exercises.

12.2 The impact on the public sector has been assessed as £5.86m over the 10 year appraisal period in the Department's central estimate for the cost of enforcing the product security regime to which this instrument relates.

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

13. Regulating small business

13.1 The legislation applies to activities that are undertaken by small businesses.

13.2 To minimise the impact of the requirements on small businesses (employing up to 50 people), the approach taken is to take into consideration any potentially disproportionate impact on small businesses when determining the most appropriate enforcement response to instances of non-compliance. Tailored guidance to assist these businesses in adjusting their business practices will also be made available.

13.3 The basis for the final decision on the most appropriate action to assist small businesses was informed by several rounds of industry consultation, alongside the Department's assessment of the relevant supply chains as well as the product security regime's impacts on them. Small businesses comprise a material proportion of connectable product retailers and excepting them altogether would significantly impede the effectiveness of this instrument and undermine the overall objectives of the regime. The Department has already assessed (see section 8B of the Impact Assessment) and will actively monitor the impact of this instrument on small businesses. The Department will ensure that the mitigations described in the preceding paragraph are used to minimise disproportionate costs as far as is appropriate without compromising the regime's effectiveness.

14. Monitoring & review

14.1 The approach to monitoring of this legislation is to assess how it impacts the levels of compliance against the three security requirements this instrument mandates, as, in the view of the National Cyber Security Centre, they will make "the most fundamental difference" in reducing vulnerabilities present in UK consumer connectable products, and therefore in protecting customers from cyber crime.

14.2 Compliance data will be gathered from the enforcement authority, and supplemented with external evidence from industry. Bespoke research concerning the cyber security threats posed by consumer connectable products, and the harms that can eventuate from them being compromised, will also be commissioned by the Department. Further details are set out in section 9 of the Impact Assessment for this instrument.

14.3 A statutory review clause is included in the instrument. It requires the Secretary of State to publish a report by 29 April 2029 assessing the effectiveness of the regulatory provision included in this instrument. Thereafter, equivalent reports must be published at intervals not exceeding five years. The Department has also committed to

conducting an interim review of the effectiveness of the regime to which this instrument relates by 29 October 2026.

15. Contact

15.1 Jonathan Angwin at the Department for Science, Innovation and Technology Telephone: 07772973227 or email: jonathan.angwin1@dcms.gov.uk can be contacted with any queries regarding the instrument.

15.2 Irfan Hemani, Deputy Director for Cyber Security Policy, at the Department for Science, Innovation and Technology can confirm that this Explanatory Memorandum meets the required standard.

15.3 The Viscount Camrose at the Department for Science, Innovation and Technology can confirm that this Explanatory Memorandum meets the required standard.

Annex

Statements under the European Union (Withdrawal) Act 2018 and the European Union (Future Relationship) Act 2020

Part 1A

Table of Statements under the 2018 Act

This table sets out the statements that may be required under the 2018 Act.

Statement	Where the requirement sits	To whom it applies	What it requires
Sifting	Paragraphs 3(3), 3(7) and 17(3) and 17(7) of Schedule 7	Ministers of the Crown exercising sections 8(1) or 23(1) to make a Negative SI	Explain why the instrument should be subject to the negative procedure and, if applicable, why they disagree with the recommendation(s) of the SLSC/Sifting Committees
Appropriate-ness	Sub-paragraph (2) of paragraph 28, Schedule 7	Ministers of the Crown exercising sections 8(1) or 23(1) or jointly exercising powers in Schedule 2	A statement that the SI does no more than is appropriate.
Good Reasons	Sub-paragraph (3) of paragraph 28, Schedule 7	Ministers of the Crown exercising sections 8(1) or 23(1) or jointly exercising powers in Schedule 2	Explain the good reasons for making the instrument and that what is being done is a reasonable course of action.
Equalities	Sub-paragraphs (4) and (5) of paragraph 28, Schedule 7	Ministers of the Crown exercising sections 8(1) or 23(1) or jointly exercising powers in Schedule 2	Explain what, if any, amendment, repeals or revocations are being made to the Equalities Acts 2006 and 2010 and legislation made under them. State that the Minister has had due regard to the need to eliminate discrimination and other conduct prohibited under the Equality Act 2010.
Explanations	Sub-paragraph (6) of paragraph 28, Schedule 7	Ministers of the Crown exercising sections 8(1) or 23(1) or jointly exercising powers in Schedule 2 In addition to the statutory obligation the Government has made a political commitment to include these statements alongside all EUWA SIs	Explain the instrument, identify the relevant law before IP completion day, explain the instrument's effect on retained EU law and give information about the purpose of the instrument, e.g., whether minor or technical changes only are intended to the EU retained law.
Criminal	Sub-paragraphs (3) and (7)	Ministers of the Crown	Set out the 'good reasons' for creating a

offences	of paragraph 28, Schedule 7	exercising sections 8(1) or 23(1) or jointly exercising powers in Schedule 2 to create a criminal offence	criminal offence, and the penalty attached.
Sub-delegation	Paragraph 30, Schedule 7	Ministers of the Crown exercising section 8 or part 1 of Schedule 4 to create a legislative power exercisable not by a Minister of the Crown or a Devolved Authority by Statutory Instrument.	State why it is appropriate to create such a sub-delegated power.
Urgency	Paragraph 34, Schedule 7	Ministers of the Crown using the urgent procedure in paragraphs 5 or 19, Schedule 7.	Statement of the reasons for the Minister's opinion that the SI is urgent.
Scrutiny statement where amending regulations under 2(2) ECA 1972	Paragraph 14, Schedule 8	Anybody making an SI after IP completion day under powers conferred before the start of the 2017-19 session of Parliament which modifies subordinate legislation made under s. 2(2) ECA	Statement setting out: a) the steps which the relevant authority has taken to make the draft instrument published in accordance with paragraph 16(2), Schedule 8 available to each House of Parliament, b) containing information about the relevant authority's response to— (i) any recommendations made by a committee of either House of Parliament about the published draft instrument, and (ii) any other representations made to the relevant authority about the published draft instrument, and, c) containing any other information that the relevant authority considers appropriate in relation to the scrutiny of the instrument or draft instrument which is to be laid.
Explanations where amending regulations under 2(2) ECA 1972	Paragraph 15, Schedule 8	Anybody making an SI after IP completion day under powers outside the European Union (Withdrawal) Act 2018 which modifies subordinate legislation made under s. 2(2) ECA	Statement explaining the good reasons for modifying the instrument made under s. 2(2) ECA, identifying the relevant law before IP completion day, and explaining the instrument's effect on retained EU law.

Part 1B

Table of Statements under the 2020 Act

This table sets out the statements that may be required under the 2020 Act.

Statement	Where the requirement sits	To whom it applies	What it requires
Sifting	Paragraph 8 Schedule 5	Ministers of the Crown exercising section 31 to make a Negative SI	Explain why the instrument should be subject to the negative procedure and, if applicable, why they disagree with the recommendation(s) of the SLSC/Sifting Committees

Part 2

Statements required under the European Union (Withdrawal) 2018 Act or the European Union (Future Relationship) Act 2020

1. Explanations

1.1 The explanations statement has been made in section 7 of the main body of this explanatory memorandum.