EXPLANATORY MEMORANDUM TO

THE PRODUCT SECURITY AND TELECOMMUNICATIONS INFRASTRUCTURE (SECURITY REQUIREMENTS FOR RELEVANT CONNECTABLE PRODUCTS) (AMENDMENT) (NO. 2) REGULATIONS 2025

2025 No. [XXXX]

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.

1.2 This memorandum contains information for the Joint Committee on Statutory Instruments and the Secondary Legislation Scrutiny Committee.

2. Declaration

2.1 Liz Lloyd, 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 Irfan Hemani, Deputy Director for UK Cyber Security and Resilience Policy at the Department for Science, Innovation and Technology confirms that this Explanatory Memorandum meets the required standard.

3. Contact

3.1 Stuart Peters at the Department for Science, Innovation and Technology can be contacted by email at the following address with any queries regarding the instrument: productsecurity@dsit.gov.uk. Alternatively, the department can be contacted by telephone: 07549 206782.

Part One: Explanation, and context, of the Instrument

4. Overview of the Instrument

What does the legislation do?

4.1 The United Kingdom's product cyber security regulatory regime is made up of Part 1 of the Product Security and Telecommunications Infrastructure Act 2022 ("the 2022 Act") and the Product Security and Telecommunications Infrastructure (Security Requirements for Relevant Connectable Products) Regulations 2023, S.I. 2023/1007 ("the 2023 Regulations"). The regime will be referred to as "PSTI" hereafter. This instrument will amend the 2023 Regulations to establish two alternative routes to achieve compliance for manufacturers of products in-scope of the PSTI regime. A manufacturer of a product that meets the security standards of any level of the Singapore's Cybersecurity Labelling Scheme for IoT or level 1 of Japan's Cyber-Security Technical Assessment Requirements Labelling Scheme (JC-STAR STAR-1) will be considered 'deemed compliant' with the security requirements set out in the 2023 Regulations and the requirement for a product to be accompanied by a statement of compliance set out in the 2022 Act. This will enable the United Kingdom to work towards mutual recognition arrangements with Japan and Singapore allowing UK

manufacturers with PSTI compliant products to have accelerated access to Singapore and Japan's respective product labelling schemes.

Where does the legislation extend to, and apply?

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

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

5. Policy Context

What is being done and why?

5.1 Ensuring that digital products are designed with cyber security in mind is an important component of protecting consumers and reduces the potential for devices being accessed or used by malicious actors. This approach is shared by likeminded countries across the globe who have introduced their own legislation or voluntary schemes to drive up the security of digital devices. This proposal aims at ensuring that countries with similar requirements to the UK are recognised and, where appropriate security measures are incorporated into devices, their ability to trade with the UK and vice versa is not hindered. This aligns with the government's priorities to drive economic growth by creating a more resilient and competitive business environment. Streamlining compliance processes and reducing costs will enable businesses to thrive and expand their reach, making the United Kingdom a more attractive market for those manufacturing or selling these products.

5.2 Under the amendments to the 2023 Regulations that this instrument implements, a Japanese or Singaporean consumer connected device manufacturer, for example of smart televisions, will be able to make their product available in the United Kingdom provided they have a valid label issued by the certifying body in their home country and that the label has not expired. They will not need to separately demonstrate compliance with the UK's own security requirements, set out in Schedule 1 to the 2023 Regulations, or have their products accompanied by a statement of compliance as required by section 9 of the 2022 Act, because their qualification for the Japanese and Singaporean labelling regimes already demonstrates that they meet the UK's security requirements.

What was the previous policy, how is this different?

5.3 Currently, all manufacturers of products in-scope of the 2022 Act and the 2023 Regulations that are made available in the UK are required to comply with the security requirements set out in the 2023 Regulations. These security requirements are 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 6451[1].

5.4 Under the new provisions inserted into the 2023 Regulations by this instrument, in-scope products can also be made available in the UK if they are currently assigned a conformance label under the JC-STAR STAR-1 that is not expired or is currently awarded a valid label under any level of Singapore's Cybersecurity Labelling Scheme that is not expired. If these conditions are met the manufacturers will be treated as meeting the security requirements outlined in Schedule 1 to the 2023 Regulations and

[1] https://www.gov.uk/government/publications/etsi-industry-standard-based-on-the-code-of-practice

meeting the requirement to have the product accompanied by a statement of compliance in section 9 of the 2022 Act.

5.5 Both the Japanese and Singaporean IoT labelling schemes require manufacturers to follow a set of baseline security requirements that are based on or align with ETSI EN 303 645. The security posture of products certified under these schemes will therefore be equivalent or greater than those that comply with the PSTI regime. There is therefore no security benefit to requiring these manufacturers to also adhere to the security requirements or the requirement to have a product accompanied by a statement of compliance where they currently have labels that are not expired.

5.6 Mutual recognition will level the playing field between UK and local businesses in the Japanese and Singaporean markets. It will also reduce the burdens on UK businesses who are looking to export to Japan and Singapore, whilst maintaining the high standard of security for products sold in the UK. UK manufacturers will have the advantage of accelerated processes to the Japanese and Singaporean labelling schemes if they desire, while Japanese and Singaporean manufacturers exporting to the UK will face reduced burdens in demonstrating that they comply with the UK's PSTI requirements.

6. Legislative and Legal Context

How has the law changed?

6.1 This instrument amends Schedule 2 to the 2023 Regulations and adds JC-STAR STAR-1 and the Singapore Cybersecurity Labelling Scheme as two additional routes to meet the conditions for deemed compliance with the security requirements. It also adds Regulation 4A of, and Schedule 2A to, the 2023 Regulations, allowing products which currently are assigned or awarded a label that has not expired under those schemes to be deemed compliant with the requirement for a product to be accompanied by a statement of compliance.

Why was this approach taken to change the law?

6.2 This is the only possible approach to make the necessary changes.

7. Consultation

Summary of consultation outcome and methodology

7.1 The Government has undertaken extensive public consultation on the product security regulatory regime 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. We received feedback that our regulations should align closely with internationally agreed technical standards. The Government response to the Call for Views on Consumer Connected Product Cyber Security Legislation[2], published in April 2022, indicated the government's intention to create alternative routes to conformity. This instrument will enable the Government to do this.

7.2 The devolved administrations were engaged with during the development of both the 2022 Act and the 2023 Regulations and are aware of the Government's intention to

[2] https://www.gov.uk/government/publications/regulating-consumer-smart-product-cyber-security-government-response/government-response-to-the-call-for-views-on-consumer-connected-product-cyber-security-legislation

designate relevant standards or schemes that can be implemented in lieu of the security requirements in legislation.

8. Applicable Guidance

8.1 Both Japan[3] and Singapore[4] have produced guidance for businesses aiming to comply with their respective labelling schemes.

Part Two: Impact and the Better Regulation Framework

9. Impact Assessment

9.1 A full Impact Assessment has not been prepared for this instrument because the potential impact on business remains well below the Equivalent Annual Net Direct Cost to Business (EANDCB) threshold of £10m. The principal scope of the 2022 Act and 2023 Regulations remain the same even after the amendments made to the 2023 Regulations by this instrument, and therefore the 2023 impact assessment, including key impacts, net effects benefits and costs remain accurate. There is insufficient evidence or data to provide a quantitative assessment of this measure and therefore the analysis below is presented qualitatively, consistent with the Better Regulation Framework[5].

Impact on businesses, charities and voluntary bodies

9.2 The impact on Japanese and Singaporean businesses selling products in the UK is positive as it provides an alternative route to demonstrate compliance and make the products available in the UK without demonstrating complying with the security requirements in the 2023 Regulations or the requirement to have products accompanied by a statement of compliance. UK businesses will face reduced burdens in applying for the Japanese and Singaporean labelling schemes, which unlike the UK's PSTI regime are voluntary. Businesses from all three countries would benefit from more efficient compliance pathways, the removal of duplicative security requirements. The reduction of compliance costs will allow businesses to get their products to market faster, avoiding delays and lost opportunities. By reducing non-tariff barriers, recognition will facilitate smoother trade flows with key partners i.e. Japan and Singapore and facilitating supply chains across these markets. Also reinforcing the UK's wider trade strategy.

9.3 The legislation does impact small or micro businesses. To minimise the impact on small or micro businesses (employing up to 50 people), the approach has been taken to not add any new obligations that they must adhere to and merely provide them with the option to choose an alternative route to compliance, where it may be beneficial for them.

9.4 There is no, or no significant impact on charities or voluntary bodies. Indirect benefits may arise where these organisations rely on regulated products or participate in supply chains, as efficiency gains for manufacturers could translate into lower costs and improved access.

[3] www.ipa.go.jp/en/security/jc-star/index.html
[4] www.csa.gov.sg/our-programmes/certification-and-labelling-schemes/cybersecurity-labelling-scheme/
[5] https://assets.publishing.service.gov.uk/media/67587ba55a2e4d4b993bfa83/better-regulation-framework-guidance-2023.pdf

9.5 There is no, or no significant, impact on the public sector because the scope of the 2022 Act is limited and only captures businesses that manufacture, import or sell consumer connectable products in the UK.

10. Monitoring and review

What is the approach to monitoring and reviewing this legislation?

10.1 The instrument does not include a statutory review clause and, in line with the requirements of the Small Business, Enterprise and Employment Act 2015, Liz Lloyd has made the following statement "in my view a review provision is not appropriate for this instrument as it merely amends the 2023 Regulations which already contains a review clause at Regulation 10."

10.2 This instrument amends the 2023 Regulations which includes a review clause at regulation 10 of those Regulations.

Part Three: Statements and Matters of Particular Interest to Parliament

11. Matters of special interest to Parliament

11.1 The Regulations come into force on the date after the date they are made. The customary 21 days' notification before Regulations come into force after being made is not required for this instrument as there are no obligations arising from the amendments to the 2023 Regulations.

12. European Convention on Human Rights

12.1 The Parliamentary Under-Secretary of State for Digital Economy 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) (Amendment) (No. 2) Regulations 2025 are compatible with the Convention rights."

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").