UK product cybersecurity – PSTI Act

On 6 December 2022, the UK Government passed into law the Product Security and Telecommunication Infrastructure Act 2022, also called the PSTI Act.

The PSTI requirements

The new legislation includes measures that will introduce a set of best practice security requirements to address the most common cybersecurity vulnerabilities and concerns of consumers:

- The use of universal default and easily guessable passwords has been banned.
- Manufacturers must provide information on how to report security vulnerabilities.
- Manufacturers must provide information about product security update support periods.

This world-leading product cybersecurity regime will come into effect on 29 April 2024.

Who has responsibilities under the new act?

This new legislation sets out responsibilities for manufacturers, importers, and distributors of UK consumer connectable products, such as:

- Smart home safety devices such as smoke detectors and fire detectors
- Smart door locks
- Connected home automation devices, smart doorbells and alarm systems
- IoT base stations and hubs to which multiple devices connect
- Smart home assistants
- Smartphones
- Connected cameras (IP and CCTV)
- Wearables
- Connected fridges, washers, freezers, coffee machines
- Smart TVs and internet-connectable game consoles;
- Smart children's toys including computers
- And other similar, connected products.

Certain products are specifically exempted from the requirements of the PSTI act, such as charge points for electric vehicles, medical devices, smart meter products, and general-purpose computers (excluding those designed and intended exclusively for children under the age of 14 years).

How to comply

Manufacturers, importers, and distributors each have a duty to ensure they only supply compliant connectable products to UK consumers.

Compliance is demonstrated by accompanying relevant products with a manufacturer's Statement of Compliance, which is the manufacturer's declaration that the product complies with the three security requirements.

Compliance with the security requirements can be demonstrated by application of the relevant provisions of the standard ETSI EN 303 645.

PSTI security requirement	ETSI EN 303 645 provision
No universal default passwords	5.1-1, 5.1-2
Information on how to report security issues	5.2-1
Information on minimum security update periods	5.3-13

(Note: The PSTI regime introduces some minor additions to the ETSI EN 303 645 provisions, such as a requirement for relevant information to be published in English).

BSI is well-positioned to help manufacturers, importers, and distributors understand if products do meet the technical requirements of the PSTI, as the first UKAS-accredited, independent test laboratory for product cybersecurity testing to ETSI EN 303 645.

Enforcement

The Office for Product Safety and Standards (OPSS) is the Secretary of State's chosen enforcing authority for Part 1 of the PSTI Act 2022, to support businesses to comply, and investigate, monitor, and take robust but proportionate enforcement action against those who do not comply.

The Secretary of State's enforcement powers under the Act include the following:

- Power to issue compliance notices, stop notices, and recall notices
- Power to issue monetary penalties up to the greater of £10 million and 4% of an organization's qualifying worldwide revenue, in respect of a single, relevant breach
- Power to inform the public about a business' compliance failures; and
- Power to publish details about enforcement action against businesses.

Get in touch today and find out more

Call: **+44 (0)345 0765 606**

Email: **product.certification@bsigroup.com**

Visit: **bsigroup.com/iot**