Navigating the PSTI Act: a guide for security professionals

BY INTIGRITI · FEBRUARY 13, 2024 · LAST UPDATED ON MARCH 6, 2025

As the implementation date of the Product Security and Telecommunications Infrastructure (PSTI) Act approaches, security professionals must understand and prepare for the regulatory changes it brings.

Commencing on 29th April 2024, this legislation marks a significant milestone in product security requirements. The Act aims to enforce a minimum standard for all IoT-driven consumer products distributed within the UK market. This guide explains the PSTI Act's implications, and the steps needed to follow it correctly.

Tip! Want to know more? Attend our on-demand session 'PSTI Act decoded: Practical tips for security professionals'.

What is the PSTI Act?

What is the PSTI Act? And what does it cover?

The Product Security and Telecommunications Infrastructure (PSTI) Act is a legislative initiative introduced in the UK. Its goal is to address cybersecurity and privacy vulnerabilities associated with consumer-connected devices, often referred to as the Internet of Things (IoT). The PSTI Act comprises two main sections:

Product security

Part 1 focuses on setting minimum security requirements for consumer connectable products to safeguard against cyber threats and attacks. It mandates manufacturers, importers, and distributors to comply with specific security standards and protocols outlined in the legislation.

Telecommunications infrastructure

Part 2 aims to bolster the deployment and expansion of mobile, fiber-optic, and gigabit-capable networks across the UK. It entails legislative amendments, including changes to the Electronic Communications Code, to facilitate the development of robust telecommunications infrastructure.

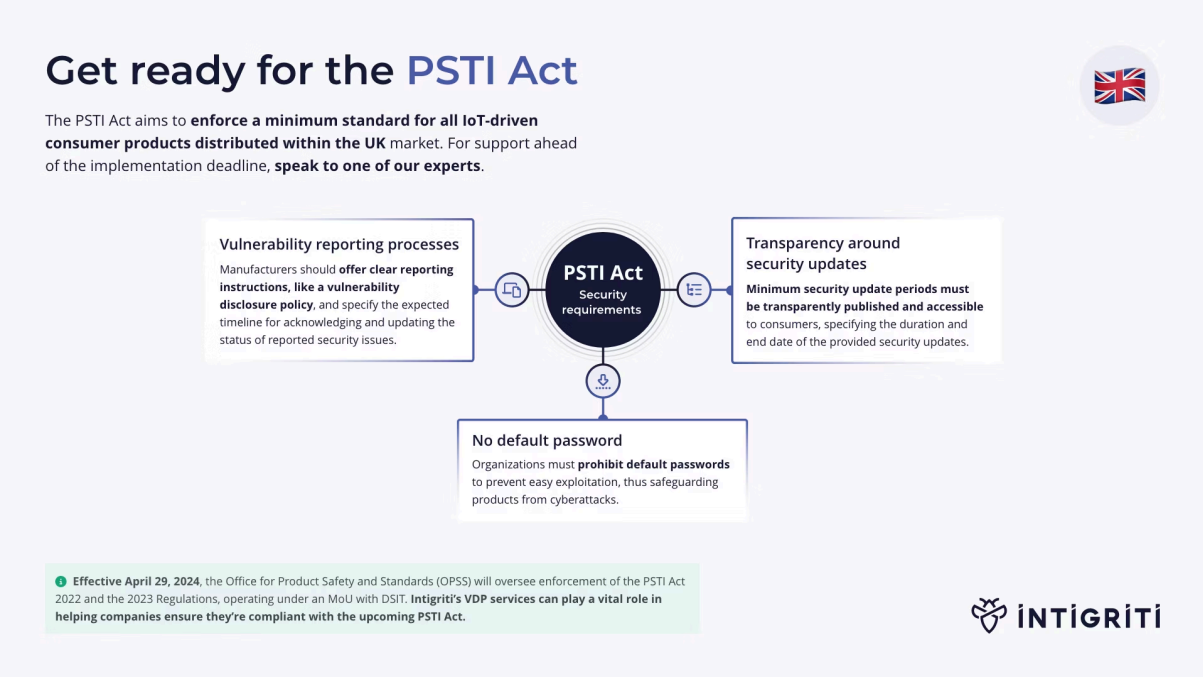
For the purpose of this article, we're focusing on Part 1 of the Act.

What are the new security requirements?

The new security requirements which are mandatory as of 29th April are as follows:

- **Prohibit the use of default passwords:** Malicious actors can easily exploit default passwords, making products vulnerable to cyberattacks.

- **Manufacturers must publish clear guidance on how to report security concerns regarding their product:** For example, through a vulnerability disclosure policy. Additionally, they should outline the expected timeline for acknowledging receipt of the report and providing status updates until the security issues are resolved for the person lodging the report.
- **Ensure transparency regarding the duration of security updates:** Consumers should be informed about how long their product will receive security updates. This bill ensures that companies must clearly state the minimum time period for providing security updates.



Who needs to comply with the PSTI Act?

Manufacturers, importers, and distributors of consumer connectable products must comply with the PSTI Act. Here is the full list of products that are impacted by the Bill:

- Smartphones
- Connected cameras, TVs and speakers
- Connected children's toys and baby monitors
- Connected safety-relevant products such as smoke detectors and door locks
- Internet of Things base stations and hubs to which multiple devices connect
- Wearable connected fitness trackers
- Outdoor leisure products, such as handheld connected GPS devices that are not wearables
- Connected home automation and alarm systems
- Connected appliances, such as washing machines and fridges
- Smart home assistants

Intigriti's Legal Counsel, explains who needs to comply with the PSTI Act

How do you ensure compliance with the PSTI Act?

The PSTI Act includes a self-declaration system which manufacturers must adhere to. You can find all the information to include in the self-declaration here. Manufacturers who don't comply with the PSTI Act risk receiving penalties, the maximum of which is either £10 million or 4% of an organization's qualifying worldwide revenue, depending on which is greater.

How can Intigriti help?

Intigriti's VDP services can play a vital role in helping companies to stay compliant with the upcoming PSTI Act. By leveraging Intigriti's platform and expertise, companies can streamline the reporting and remediation process for security vulnerabilities, ensuring compliance with the PSTI Act's requirements while bolstering their overall cybersecurity posture.

For more support, attend our free session 'PSTI Act decoded: Practical tips for security professionals'.