# IoT and PSTI

## The impact of the Product, Security and Telecommunications Infrastructure Act (PSTI 2022) on manufacturers and distributors

### What is the new security regulation for IoT Manufacturers?

The UK government has taken industry wide steps to protect consumers of IoT or Smart devices by imposing a minimum set of security requirements on IoT products.

This means that manufacturers will be found at fault if they provide non-compliant devices to customers.

And, it's not just manufacturers, the importers and distributors of devices can be found at fault too.

The definition is; 'any device connected to the internet via cellular data, Bluetooth, wifi or cable.' This means devices not normally considered as part of the IoT family, may suddenly find themselves within the scope.

Each distinct product needs to prove that it conforms to three security principles:

1. Passwords are unique per product, or defined by the user
2. Transparency is key on frequency and term of security updates
3. Contact information is published to allow product vulnerabilities to be freely reported

The PSTI act became law in April 2023. Similar to the General Data Protection Regulation, a 12-month grace period was allowed for time to ensure compliance. The effective deadline for compliance is 29th April 2024.

## What does the manufacturer need to do?

The regulation asks for a "statement of compliance" to legally permit your products to be available in the UK as a consumer-connectable product.

This must be a document that conforms to the prescribed format and states that the manufacturer has complied with the applicable IoT cybersecurity requirements of the PSTI.

As the penalties can be considerable it is crucial that the 'statement' is accurate as well as comprehensive.

## What happens if they ignore it?

With the OPSS (Office for Product, Safety and Standards) ensuring compliance there is the very real risk of product recall and worse, heavy fines for those who do not adhere to the new regulation.

1. A compliance notice will be received outlining the shortcomings in the manufacturers current approach
2. A Stop Notice will be issued detailing specific steps needed or requesting evidence of compliance. It may require them to inform customers of potential risks and demand a proof of compliance by a certain date
3. A recall notice can be issued that requires the manufacturer or distributor to make arrangements for a product-wide return of the offending devices
4. If the above actions are not followed to satisfaction then, a maximum fine of £10 million or up to 4% of the company's worldwide revenue can be levied

## What can we do about it?

IASME IoT Baseline standard certificate has been confirmed by DSIT (Department of Science, Innovation and Technology) as a valid statement of compliance.

Achieving the certification through an independent assessment body in advance of the deadline allows organisations to de-risk the process of investigation and enforcement by providing advanced confirmation that the device is compliant with the Act.

Importers and distributers likely to be handling vast numbers of IoT products may also wish to use the scheme as a simple way to ensure that devices that they are selling to consumers meet the standard and therefore avoid enforcement action themselves.

A ADVISE C CERTIFY T TEST

# CONTACT OUR TEAM


0161 513 0960

secarma.com

enquiries@secarma.com