Department for
Science, Innovation
& Technology

PSTI (Product Security) regime - overview

Overview of the PSTI regime

Overview of the **PSTI (Product Security) regime** (1/2)

PSTI regime

Overview of PSTI regime

Detailed view of initial security baseline

Legislation scope
Role of economic actors
How it will be enforced
Outcomes

Legislation scope

Defining products in scope

*The legislation applies to any **consumer connectable products and their associated services.***

Excepted product classes

*Specific product classes that would otherwise fall within the scope of this legislation, but for which it would be inappropriate for it to apply to, **will be exempted.***

Adaptable scope

*Ministers, subject to agreement by Parliament, can **adjust the scope of products covered by this regulation.***

Interoperability

*The legislation is **interoperable** with other existing or planned government interventions covering contiguous, or overlapping product classes.*

Role of economic actors

Obligations

*The legislation places **proportionate obligations on relevant economic actors** involved in the transmission of in scope products to consumers.*

Security Requirements

*The legislation will obligate industry to not make products available unless they **comply with certain security requirements set out in secondary legislation.***

Adaptable requirements

*The legislation allows Ministers to **update the security requirements and conditions for deemed compliance.***

Product Assurance

*The legislation enable Ministers to **mandate product assurance** for particular categories of consumer connected products.*

How it will be enforced

Enforcement authority

*The **Office for Product Safety and Standards** will investigate and take action against non-compliance, and support industry to comply.*

Enforcement authority role

*The legislation equips the authority with **necessary powers** as well as the ability to issue corrective measures, sanctions, and possible criminal proceedings.*

Appeals

*Relevant economic actors will have the right to **appeal any sanction or corrective measure** brought against them.*

Proportionate transition

*Government will provide a **12 month transition period** for businesses to adjust their business practices.*

Outcomes

- ✔ ***Protecting citizens, networks and infrastructure from harm;***
- ✔ ***Enabling emerging tech to innovate, grow and flourish by improving security, and increasing consumer confidence;***
- ✔ ***Adopting a proportionate approach, without compromising effectiveness;***
- ✔ ***Continuing to protect citizens, networks and infrastructures from harm in the face of an uncertain future.***

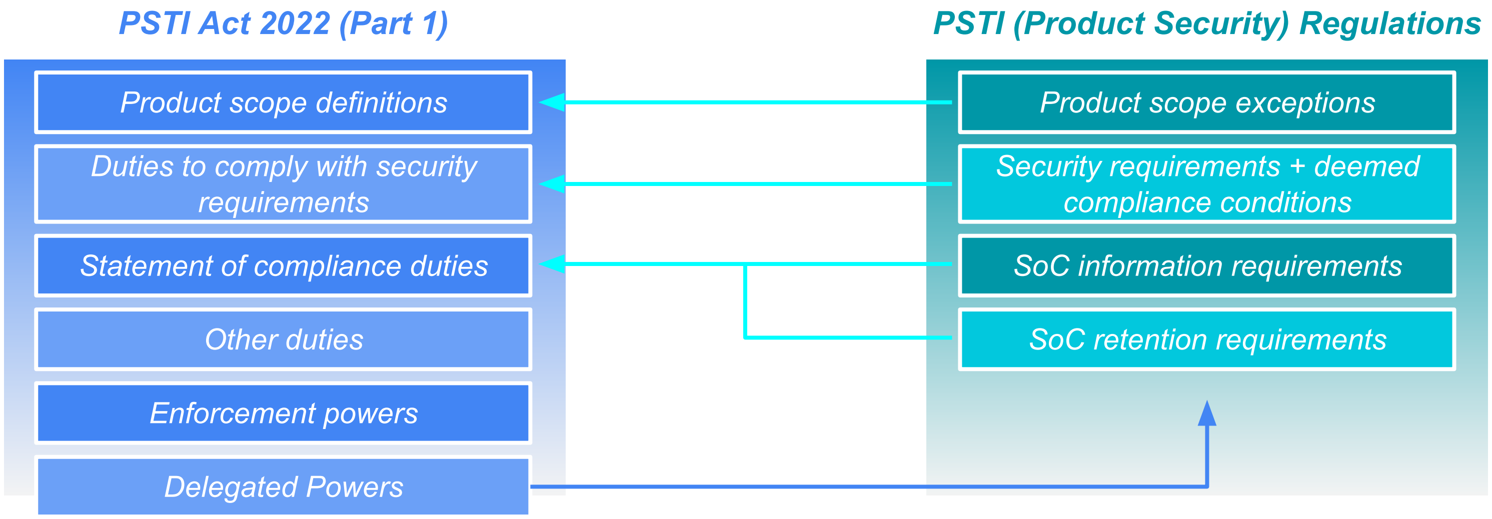
Overview of the **PSTI (Product Security) regime** (2/2)

PSTI regime

Overview of PSTI regime

Detailed view of initial security baseline

- The PSTI (Product Security) regime is underpinned by extensive industry engagement, including a **Consultation (2019)** and **Call for Views (2020)**.
- The Government detailed it's final intentions for the regime in it's **Call for Views Response (2021)**.
- The regime will be delivered across two pieces of legislation:



PSTI Act 2022 (Part 1)

Product scope definitions

Duties to comply with security requirements

Statement of compliance duties

Other duties

Enforcement powers

Delegated Powers

PSTI (Product Security) Regulations

Product scope exceptions

Security requirements + deemed compliance conditions

SoC information requirements

SoC retention requirements

Regime Implementation

Department for
Science, Innovation
& Technology

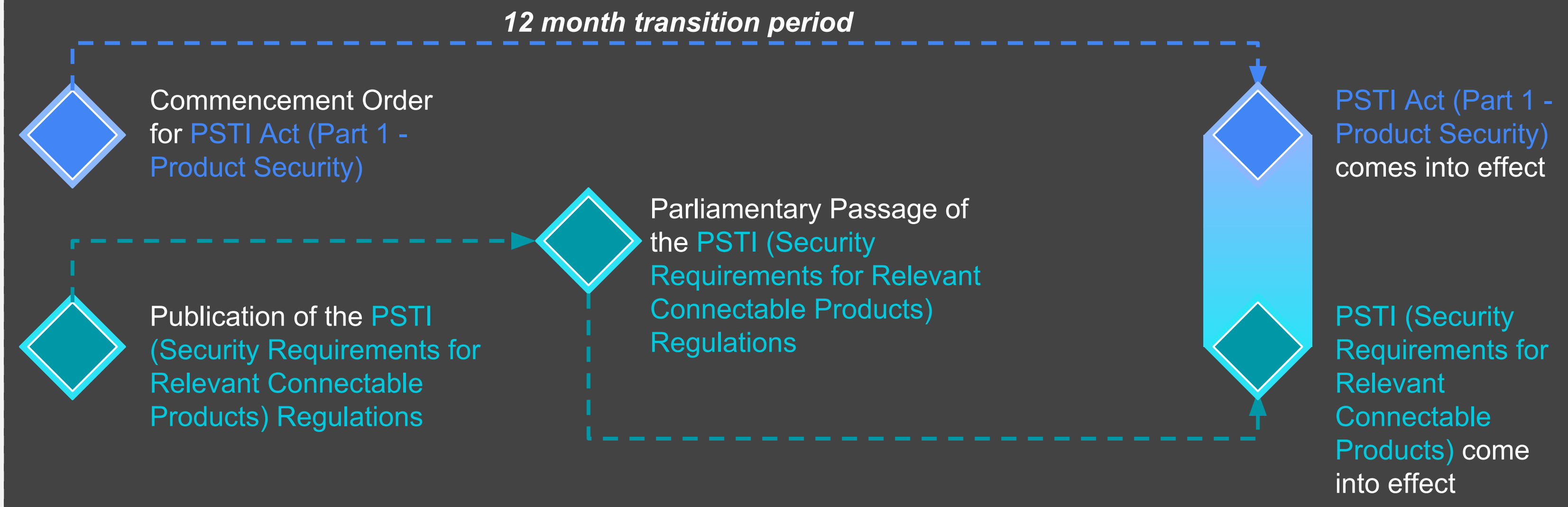
PSTI regime

Overview of PSTI regime

Detailed view of initial security baseline

- The Government has published the draft secondary legislation required to bring the PSTI (Product Security) regime into force. This sets out the security requirements that manufacturers will need to comply with.
- This legislation was published on 29 April 2023 triggering the start of a 12 month transition period before the PSTI (Product Security) regime comes into effect on **29 April 2024**.

Implementation process



12 month transition period

Commencement Order for PSTI Act (Part 1 - Product Security)

Publication of the PSTI (Security Requirements for Relevant Connectable Products) Regulations

Parliamentary Passage of the PSTI (Security Requirements for Relevant Connectable Products) Regulations

PSTI Act (Part 1 - Product Security) comes into effect

PSTI (Security Requirements for Relevant Connectable Products) come into effect

Detailed view of initial security baseline

Overview of the **PSTI (Product Security) security baseline**

PSTI regime

Overview of PSTI regime

Detailed view of initial security baseline

- The initial security baseline will **apply to manufacturers**, and, with the exception of security requirement 1, **extend to software that may not be installed on the physical device**, or be provided by a manufacturer of the product.

			Requirement scope			
	Persons subject to the requirement	Category	Hardware	Software pre-installed	Fundamental software	Associated software
Security Requirement 1 *Ban universal default (and easily guessable) passwords* *(ETSI EN 303 645 5.1-1 + 5.1-2)*	*Manufacturers*	*Technical product requirement*	✓*	✓*	✓*	
Security Requirement 2 *Publish information on how to report security issues* *(ETSI EN 303 645 5.2-1)*	*Manufacturers*	*Organisational action*	✓	✓	✓	✓*
Security Requirement 3 *Publish information on minimum security update periods* *(ETSI EN 303 645 5.3-13)*	*Manufacturers*	*Organisational action*	✓ *	✓ *	✓ *	✓ *

! **Note -** The requirements, and definitions of the software it would be proportionate to capture within each requirement will be set out in secondary legislation

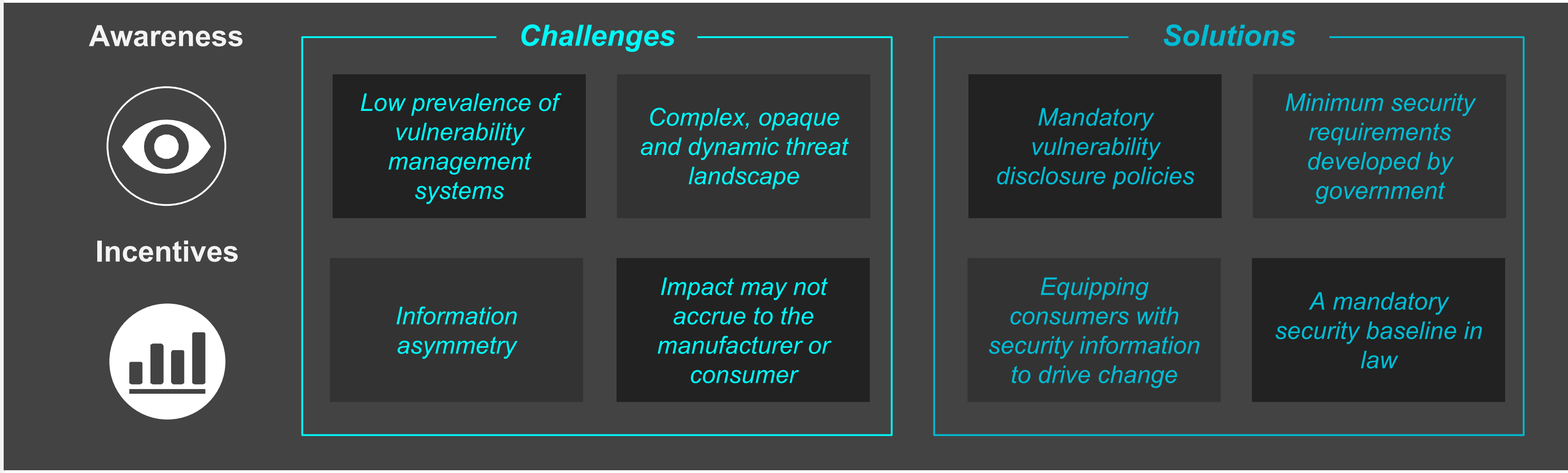
Why these security requirements?

PSTI regime

Overview of PSTI regime

Detailed view of initial security baseline

- Improving the cyber-security of consumer connectable products requires the manufacturers of these products to be:
  - ***Aware of vulnerabilities*** *in their products and how malicious actors may exploit them; and*
  - ***Appropriately incentivised*** *to address vulnerabilities and implement security measures*



	Challenges		***Solutions***	
Awareness	*Low prevalence of vulnerability management systems*	*Complex, opaque and dynamic threat landscape*	*Mandatory vulnerability disclosure policies*	*Minimum security requirements developed by government*
Incentives	*Information asymmetry*	*Impact may not accrue to the manufacturer or consumer*	*Equipping consumers with security information to drive change*	*A mandatory security baseline in law*

Impact of the top three Code of Practice guidelines
NCSC Statement 1 (PSTI Act Impact Assessment)

> *"The NCSC's view is that the top three principles within the Code of Practice and ETSI EN 303 645 will make the most fundamental difference to the vulnerability of consumer connectable products in the UK, are proportionate given the threats, and universally applicable to devices within scope. While the other requirements in the Code of Practice and EN 303 645 could reduce the potential vulnerabilities that may be discovered in a device, if those vulnerabilities can't be easily reported, and users don't know if their device can still receive updates then devices will remain at high risk. In this situation, the other requirements would make minimal difference."*