ETSI
The Standards People

Security Conference

From Standards to the UK Product Security Regime: Legislation and Enforcement

Presented by:

Veena Dholiwar &
Warda Hassan

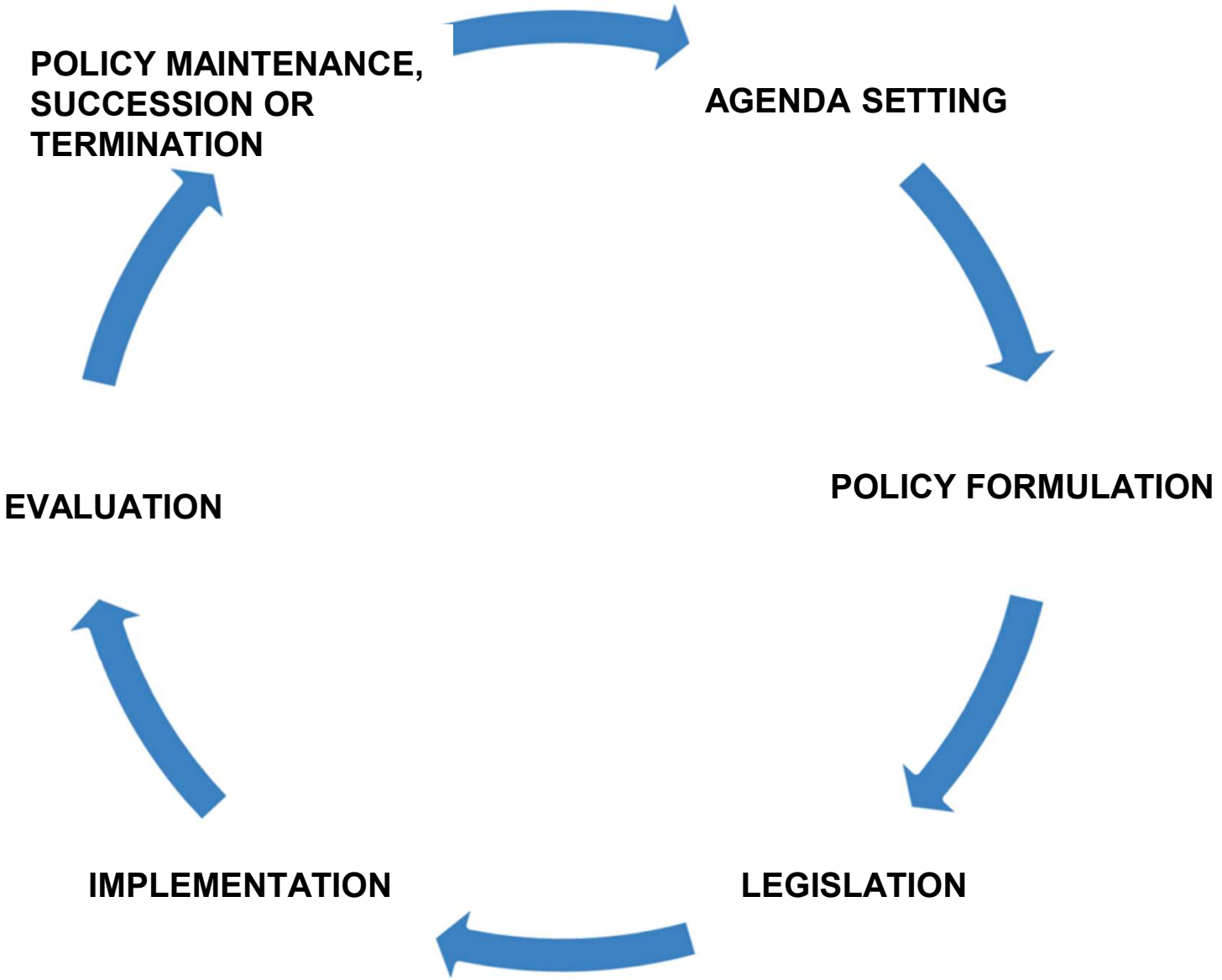
Department for
Science, Innovation
& Technology

Overview of the **PSTI (Product Security) Regime**

The PSTI Regulations 2023 will come into effect on 29 April 2024, following a 12 month transition period, requiring manufacturers, importers and distributors of consumer connectable / IoT products to comply with minimum security requirements. From April 2024, the relevant parties obligated under the legislation will be required to comply with the security requirements below;

1. Banning **universal and easily guessable default passwords** on consumer connectable products
2. Manufacturers must have a readily available **public point of contact for reporting vulnerabilities**
3. Transparency with consumers on the **minimum length of time they will receive security updates**

The scope of our work on consumer IoT security to date: 2018-2023



Timeline: **PSTI (Product Security) Regime**

Department for Science, Innovation & Technology

2018

- ✓ ***March:*** *Code of Practice for Consumer IoT Security published in draft.*
- ✓ ***October:*** *Code of Practice for Consumer IoT Security published in eight languages*

2019

- ✓ ***May:*** *Consultation launched for regulatory proposals*

2020

- ✓ ***January:*** *Consultation response published and intention to legislate announced*
- ✓ ***July:*** *Call for Views published on proposals for regulating consumer connected products*

2021

- ✓ ***April:*** *Government response to call for views published*
- ✓ ***November:*** *PSTI Act introduced into the House of Commons*

2022

- ✓ ***May:*** *PSTI Act introduced into the House of Lords*
- ✓ ***December:*** *PSTI Act receives Royal Assent*

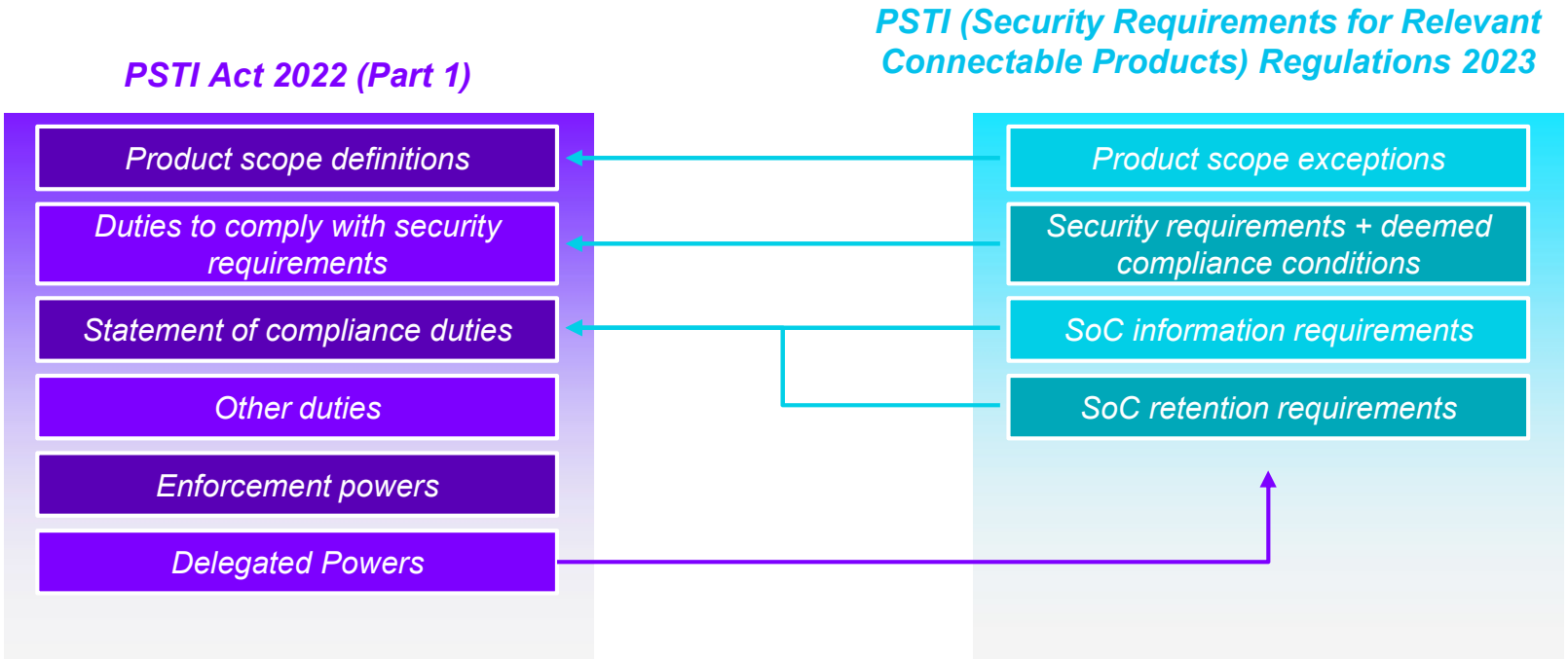
2023

- ✓ ***29 April:*** *Draft Product Security Regulations Published*
- ✓ ***13 September*** *Product Security regulations approved by Parliament*

artment for
nce, Innovation
chnology

Overview of the **PSTI (Product Security) Regime**

- The UK's new product security regime will be the **first in the world** to require minimum cyber security requirements before consumer connectable products are made available for sale to UK customers.
- The Product Security and Telecommunications Infrastructure Act received Royal Assent on 6 December 2022.
- The Product Security Regulations 2023 were laid in Parliament on 10 July and approved on 13th September.
- The **UK's product security regime comes into force on 29th April 2024.**



PSTI (Product Security) Regime: Deemed Compliance

PSTI (Security Requirements for Relevant Connectable Products) Regulations 2023	ETSI EN 303 645
SCHEDULE 2	**Conditions for deemed Compliance**
SR1: Passwords	Provisions 5.1-1 & 5.1-2
SR2: Information on how to report security issues	Provisions 5.2-1 or paragraphs 6.2.2, 6.2.5 & 6.5 of ISO/IEC 29147
SR3: Information on minimum security update periods	Provisions 5.1-1 & 5.1-2

Next steps: Enforcement

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

Enforcement will be risk based and proportionate with a focus on supporting businesses to achieve compliance.

OPSS will carry out their activities in a targeted, proportionate, consistent, transparent and accountable manner, in accordance with the Regulators' Code.

Activities will include

- Awareness raising
- Business engagement
- Intelligence Building
- Monitoring and Intervention
- Guidance and Resources
- Reporting

Department for Science, Innovation & Technology

PSTI (Product Security) regime - Enforcement Notices and Sanctions

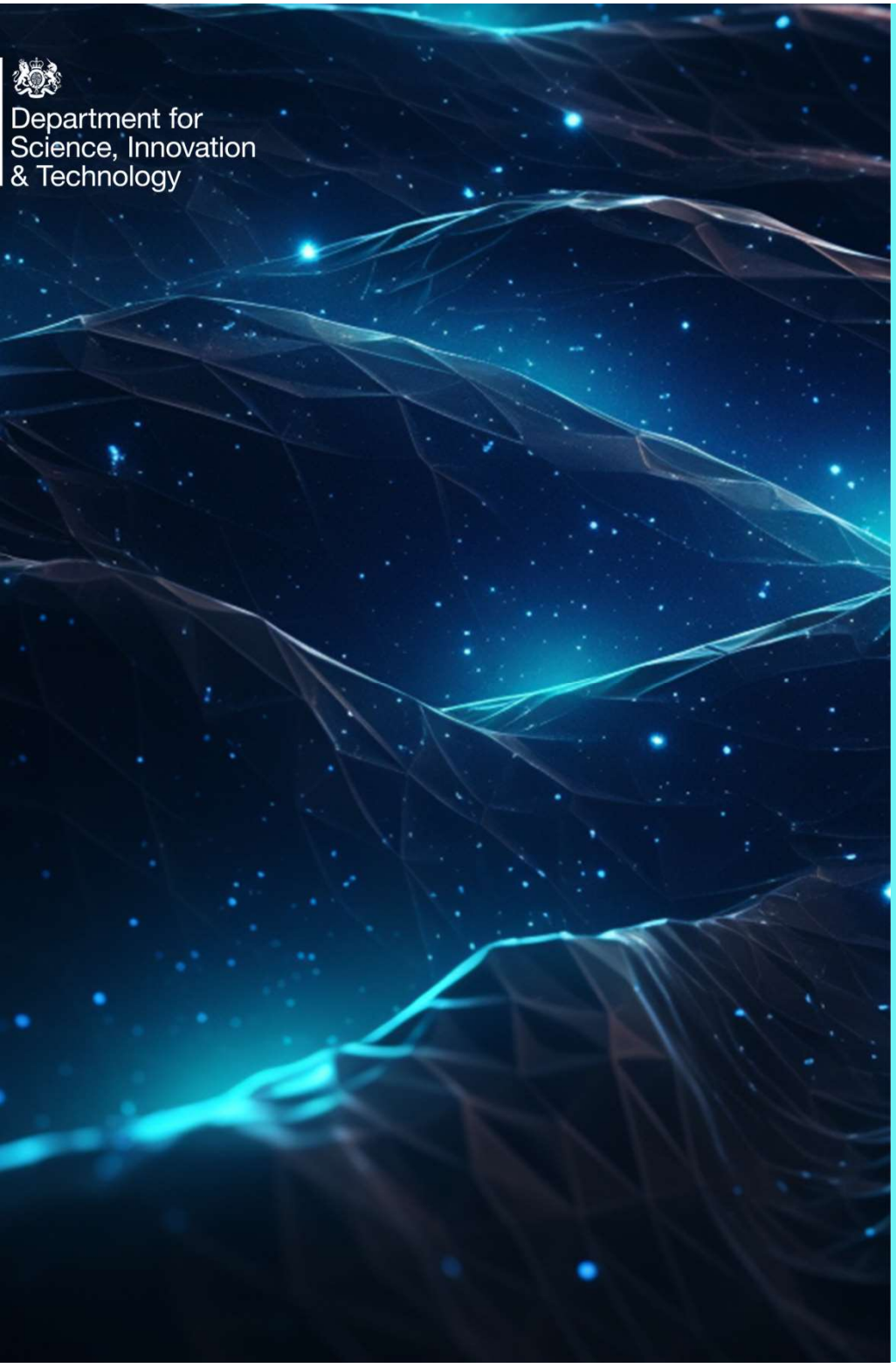
Corrective Measure	Description
Compliance Notice	*A notice requiring a person to comply with the relevant duty within a specified period.*
Stop Notice	*A notice requiring a person to stop carrying on a specified activity within a specified period if there are reasonable grounds to believe that non compliance is/ will continue*
Recall Notice	*A notice requiring a person to make arrangements for the return of the products to themselves or to another person, if reasonable grounds to believe that there is a compliance failure relating to products already supplied to customer. E.g if action taken is inadequate or if a Compliance/Stop Notice/Forfeiture is not adequate to sufficiently manage risks*
Forfeiture	*If the SoS has reasonable grounds to believe that there is a compliance failure relating to any forfeitable products the SoS may apply to the appropriate court for a forfeiture order and the products to be given to a specified person to be disposed of or destroyed.*
Monetary Penalty	*If SoS is satisfied on the balance of probabilities that there has been a compliance failure, they may issue a penalty that is the greater of £10 million, and 4% of the person's qualifying worldwide revenue and may require the person to pay £20,000 a day for continuing breaches*
Offences	*Non-compliance with an enforcement notice* *Obstructing an enforcement officer* *Purporting to act as an enforcement officer*

Research & Evaluation

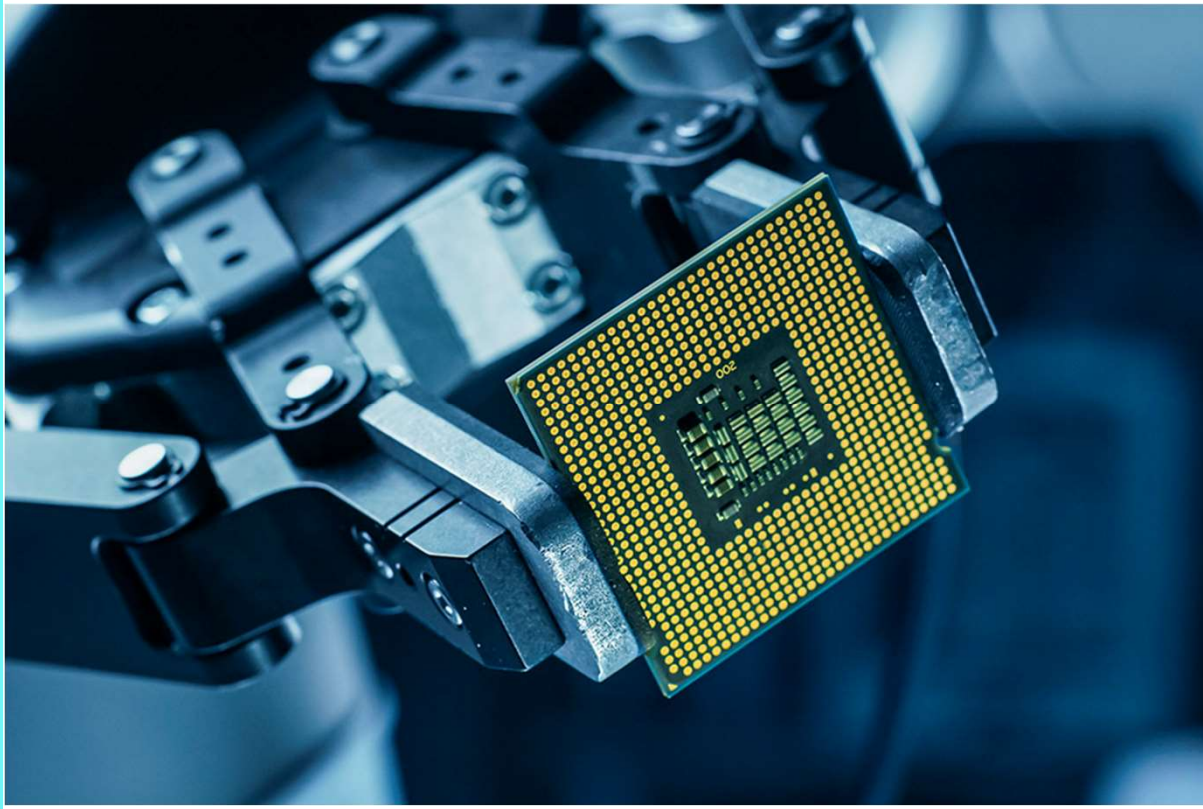
- Analysing and evaluating the consumer IoT landscape to assess the impact of legislation.
- Measuring the impact on consumers and businesses.
- Identifying and evidencing next steps.

Introduction to DSIT

- Coming together of science, innovation and technology
- UK's National Cyber Strategy 2022
- UK's International Technology Strategy
- AI Regulations White Paper
- Science and Technology Framework: Priority Technologies
  - Artificial Intelligence
  - Engineering Biology
  - Future Telecommunications
  - Semiconductors
  - Quantum Technologies



National Cyber Strategy & Pillar 3 Technology Advantage



The Cyber Technology Landscape

- Enterprise IoT
- Operational Tech
- App Store Security
- Software Resilience
- Connected Places

Emerging Technology

- AI
- Quantum
- Semiconductors
- Digital Twins
- Engineering Biology

Department for Science, Innovation & Technology

Questions and Contact Details

Department for Science, Innovation and Technology

Veena.Dholiwar@dsit.gov.uk or
Warda.hassan@dsit.gov.uk