

Product Security and Telecommunications Infrastructure Bill

AMENDMENT
TO BE MOVED
ON REPORT

Clause 1

LORD CLEMENT-JONES

Page 1, line 17, at end insert—

- “(2A) Regulations under this section must, among other things, include security requirements that—
- (a) prohibit the setting of universal default passwords and the ability to set weak or easily guessable passwords;
 - (b) require the production and maintenance by manufacturers of regular publicly-available reports of security vulnerabilities;
 - (c) ensure the provision of information to the consumer, before the contract for the sale or supply of a relevant connectable product is made, detailing the minimum length of time for which the consumer will receive software or other relevant updates for that product;
 - (d) introduce appropriate minimum periods for the provision of security updates and support, taking into account factors including the reasonable expectations of consumers, the type and purpose of the connectable products concerned and any other relevant considerations.
- (2B) Regulations under this section must include provision that all security requirements specified in accordance with this Act are included as essential requirements in statutory conformity assessments and marking procedures under the Radio Equipment Regulations 2017 (S.I. 2017/1206), and in any other such assessments and procedures applicable to relevant connectable products.”

Member’s explanatory statement

This amendment expressly sets out on the face of the Bill security requirements, which this bill seeks to establish through future regulations, providing specific legal guidance regarding the individual security requirements and obligations on relevant parties.

Product Security and Telecommunications Infrastructure Bill

AMENDMENT
TO BE MOVED
ON REPORT

6 October 2022
