Department for Digital, Culture, Media & Sport

Julia Lopez MP
Minister of State for Media, Data
and Digital Infrastructure
4th Floor
100 Parliament Street
London SW1A 2BQ

E: enquiries@dcms.gov.uk

www.gov.uk/dcms

Chris Elmore MP
House of Commons
London
SW1A 0AA

5 April 2022

MC202/05077/DC

Dear Chris,

I am writing in regard to the Product Security and Telecommunications Infrastructure Bill which completed its Public Bill Committee on 22 March. I was pleased to see cross-Party support for the Bill which will improve both the security of UK consumer connectable devices and support the roll-out of digital infrastructure.

I am writing to follow up on a small number of matters raised at the Committee which I set out below. I am copying this letter to the other Committee members.

Cyber security reporting periods and obligations
You asked for further information about the obligations of the Secretary of State and Accounting Officer, as well as regular reporting cycles the product security aspect of this legislation will consider.

The government will review the security requirements and other regulations made using the powers provided by this Bill as required as per our obligations under section 28 of the Small Business, Enterprise and Employment Act 2015. This Act requires regulations affecting business to be subject to periodic review, which is generally no longer than 5 years after the regulation comes into force. Such a review will take whatever form is most appropriate, be it formal or informal. These requirements are, of course, in addition to regular scrutiny that Parliament gives to the government's National Cyber Strategy. The product security measures in this Bill are core to the delivery of the technology pillar of the strategy. The Public Accounts Committee, the Intelligence and Security Committee, and the Joint Committee on National Security Strategy, regularly hold the government to account on its delivery of the National Cyber Strategy.

The government also regularly produces reports on security risks across a range of technologies, including consumer connectable products. This includes regular progress reports on the National Cyber Strategy overall, the annual DCMS-commissioned Cyber Breaches Survey, as well as the NCSC annual report. The latter is separate to the National Technical Authority's weekly and monthly threat and vulnerability assessment reports.

Impact on business regarding disposal of devices
I can confirm that the government's central estimate for the cost to business of this legislation over 10 years is £1246.9m, though this is significantly outweighed by the economic and social benefits generated. The Hon. Member for Cardiff West further asked for more information on the Product Security impact assessment's range of figures referring to the percentage of stock that may be disposed of by businesses as a result of this legislation coming into force.

The methodology considered a range of information and assumptions. This was difficult given two primary uncertainties at the time of writing: (i) the practicalities of manufacturers addressing compliance failures in their products, and (ii) the potential response of business to the legislation. As a starting point, research showed that around 10% of assessed products already in stock, and intended for UK consumers, had default passwords. This provided a conservative baseline of the retail stock of consumer connected devices that will be disposed of, given non-compliance. There is a chance this could be even lower given software updates, or similar means, can be used to address the default passwords compliance failures. Further the additional security requirements around a vulnerability disclosure policy and transparency on security updates, are considered relatively straightforward for the manufacturer to embed to ensure compliance of their product.

We are confident that industry will embrace these requirements, and this informs our optimistic consideration of 5%. As is appropriate for this type of assessment, we have also considered the potential impact of notable manufacturer difficulties in addressing compliance failures, and significant industry non-adherence, to inform this worse case scenario figure of 45%. We have robustly mitigated the latter by bringing industry with us, as we developed the legislative approach, and are confident in our central estimate of 10% as a reasonable baseline to inform this assessment. We will, of course, continue to work with industry partners to explore whether we can reduce the risk of unnecessary device disposal even further, while progressing this security requirement baseline.

Clause 57
I would also like to take the opportunity to provide some additional information following the Committee's discussion on clause 57 of the Bill. This clause is intended to ensure that operators are not prevented from getting rights they need to maintain their networks simply because they are already in occupation of land.

At the moment this is not always possible. This is because new Code rights can normally only be granted by whoever is occupying the land that any apparatus is to be kept on. This works in relation to entirely new agreements. But in some cases, for example, where an operator has already installed their equipment, under an expired or ongoing agreement, they may effectively be the occupier of that land. Clearly, in those circumstances, the operator cannot grant themselves new rights. In practice, this would mean the only feasible way these operators could get new rights would be by removing their apparatus, vacating the land and then asking for the rights again. Not only would this be a waste of resources, it could also lead to unnecessary service disruptions.

The changes we are making mean operators who are occupying land will be able to ask for the rights that they need from whoever would be in a position to grant those rights, if the operator was not occupying the land. In the Bill this person is identified as being any person (other than the operator) who exercises powers of management or control over the land. In most cases, that will be the landowner, or the person with whom the operator already has an agreement. There may be some situations where no one exercises powers of management or control over the land. In those circumstances, the operator will be able to ask for Code rights from any person with an interest in the land that would be prejudicially affected by the

exercise of a Code right. This is set out in clause 57 and will be contained in the new sub-paragraph (6B) of paragraph 105 of the Code.

I should add that stakeholders have raised concerns that clause 57 in its current form may have unintended consequences. We are looking at this closely and, if necessary, will bring forward amendments to ensure the policy aim of this clause is achieved.

I will place a copy of this letter in the Libraries of both Houses.

With best wishes,

Julia Lopez MP
Minister of State
Minister for Media, Data and Digital Infrastructure

Copied to Public Bill Committee members:

Simon Baynes MP, Saqib Bhatti MP, Kevin Brennan MP, Steve Double MP, Ruth Edwards MP, James Grundy MP, Sally-Ann Hart MP, Kate Hollern MP, Rebecca Long Bailey MP, Navendu Mishra MP, Kate Osbourne MP, Tom Randall MP, Shailesh Vara MP, David Warburton MP, Mick Whitley MP