Department for
Digital, Culture
Media & Sport

Matt Warman MP
Minister for Digital Infrastructure
4th Floor
100 Parliament Street
London SW1A 2BQ

www.gov.uk/dcms
enquiries@dcms.gov.uk

Chi Onwurah MP
House of Commons
London
SW1A 0AA

INT2021/01792/DC
26 January 2021

Dear Chi,

TELECOMMUNICATIONS SECURITY BILL - COMMONS COMMITTEE STAGE

Thank you for your thoughtful contributions during the Bill's scrutiny sessions on 21 January. As I said during the debate, I am encouraged that we are aligned on the majority of the Bill's provisions and I look forward to continuing our close working relationship to ensure the passage of this vital piece of legislation as soon as possible. I committed to write to you and the Rt Hon Member for North Durham on a number of areas. I have set out further detail on these areas in this letter.

Duties to take security measures

During the committee session on 21 January, you asked for clarification on the relationship between the new overarching security duties in the Bill and the specified security measures to be contained in regulations. You also sought clarity on how the NCSC technical guidance that will form the basis of codes of practice will align with those regulations.

I should first summarise the duties to take security measures placed on providers of public electronic communications networks and services by the Bill. New section 105A (inserted by clause 1) requires providers to take appropriate and proportionate measures for the purposes of identifying and reducing the risks of security compromises occurring, and preparing for any occurrence of security compromises. New section 105C (inserted by clause 2) requires providers to take appropriate and proportionate measures in response to any security compromises that do occur, to limit their adverse consequences or mitigate any adverse effects on the network or service.

These are broad duties that require providers to take responsibility for ensuring the security and resilience of their networks and services. However, the Bill also confers power on the Secretary of State to make regulations under new sections 105B and 105D to supplement these duties by requiring providers to take specified security measures or measures in response to a security compromise. Any such measures do not affect providers' broad duties imposed by the Bill.

New section 105E (inserted by clause 3) enables the Secretary of State to issue codes of practice giving guidance as to the measures to be taken by providers to meet their duties under section 105A and 105C, or as specified in regulations.

It has always been our intention that the new security framework should provide clarity to industry, whilst providing the necessary flexibility and powers for the government to respond appropriately as risks and technology change. The approach in this Bill - with its combination of strengthened security duties, specific requirements in secondary legislation, and codes of practice to offer technical guidance - allows us to do all those things.

Audit

In the debate on amendment 8 of the Bill, you asked whether network providers would be required to carry out an audit of the equipment used in their networks.

Telecoms providers need to be aware of the equipment within their networks in order to fully understand the risks to those networks. New section 105A requires providers to take appropriate measures to identify the risks of security compromises occurring and such measures would of course include assessing which equipment used within the network might be vulnerable to attack. However, we intend to make further provision in regulations under new section 105B.

As members of the Committee are aware, the Government has published an early draft of those regulations for engagement with providers. These will be revised further over the coming months as we receive feedback from industry on the specific requirements. These draft regulations include measures to ensure providers identify, record and reduce the risk of security compromises as well as ensure proper oversight of their supply chain security. Requirements are also included to ensure secure network architecture (draft regulation 3), monitoring and audit (draft regulation 5) and measures addressing the security of supply chains (draft regulation 6). I hope the draft regulations demonstrate our intention to ensure that providers are required by law to carry out appropriate audits of their networks.

Codes of practice will provide further guidance on the steps to take to ensure compliance with the law, including with respect to auditing. Codes will apply to certain providers and will be subject to a public consultation. Codes of practice will be updated as new threats emerge and technologies evolve. Members have been provided with a copy of draft NCSC technical guidance that will form the basis of a Government-issued code of practice, and can see this contains detailed guidance on how to maintain audits as part of good security practices.

Insofar as your concern relates specifically to equipment manufactured by a designated or high-risk vendor, I should also note that the Bill enables the Secretary of State to require providers to submit plans setting out the steps they will take to comply with requirements in a designated vendor direction (clause 15). In the case of a requirement to remove equipment this would include any steps needed to establish which equipment needed to be removed. The Bill also enables Ofcom to carry out surveys of a network or service to gather information on a provider's compliance with requirements in a designated vendor direction (clause 19). Alongside this, clause 23 enables the Secretary of State to require the provision of information about the use of goods, services or facilities supplied, provided or made available by a particular person. I look forward to debating these clauses later this week.

NCSC and OFCOM statement

As the UK's cyber security agency, the National Cyber Security Centre has been fundamental to the development of this Bill, and will continue to be fundamental to its implementation. This work builds on a longstanding relationship between the NCSC, Ofcom and DCMS on matters related to cyber security.

You asked for further information explaining NCSC's role in the Bill's implementation, with reference to the statement NCSC and Ofcom will soon be publishing setting out how they will work together.

NCSC, as part of GCHQ, has an existing statutory remit under the Intelligence Services Act 1994 to provide technical security advice, and can receive information on telecoms security for the purpose of exercising that function. It is under that existing statutory remit that the NCSC provided the comprehensive security analysis underpinning the Telecoms Supply Chain Review; provided guidance to public telecoms providers on how to manage the risks posed by high risk vendors; and through detailed threat modelling created the Telecoms Security Requirements that will form the basis of an initial code of practice, as I have already mentioned.

The NCSC will provide expert advice to Ofcom, in accordance with that remit, to support Ofcom's monitoring, assessment and enforcement of the new security framework. NCSC and Ofcom are currently working to agree a memorandum of understanding that will ensure each organisation's respective roles are clear. This reflects the approach that NCSC has taken with other regulators to agree arrangements for collaborative working which respect some of the fundamental principles of the NCSC's operating model, namely that they themselves are not a regulator, and that any cooperation with regulators does not adversely impact NCSC's relationships with the companies they advise on security.

NCSC and Ofcom intend to publish a statement prior to the bill's report stage providing more details of how they will work together, and setting out the high level principles expected to underlie the memorandum of understanding. Whilst not a legal document, the statement will include information on their respective roles as well as their approach to information sharing. The statement and memorandum of understanding will demonstrate the intent of Ofcom and NCSC and the detailed work that the two organisations have done to agree and clarify their changing roles under the new regime.

The memorandum of understanding will not be put in the public domain. This approach is consistent with the approach NCSC takes with other sectoral regulators and will provide NCSC the flexibility to continue to provide advice to both public telecoms providers and regulators in accordance with its remit. I hope this provides reassurance that NCSC will continue to play a vital role in ensuring telecoms security and that Ofcom and NCSC are committed to working together in our national interest on this matter.

Informing users of security compromises

In the debate on clause 4, you queried the interaction between the reporting duties set out in that clause and data breach reporting under the UK's data protection legislation.

New section 105L enables Ofcom to inform users of a network or service about the occurrence of a security compromise, and of any technical measures those users can take to protect themselves or to mitigate any adverse effect on them. Ofcom may also require the relevant provider to inform their users of these matters.

In some cases, a security compromise may also constitute or result in a personal data breach. Article 34 of the UK General Data Protection Regulation (GDPR) sets out the circumstances in which a data controller must communicate a personal data breach to the individuals affected. When the breach is likely to result in a high risk to their rights and freedoms, the controller must communicate the breach to them without undue delay unless certain exceptions apply. The communication should describe in clear and plain language the nature and likely consequences of the breach; provide a contact point for them to obtain more information; and describe the measures taken or proposed to address the breach or mitigate its effects. Regulation 5A of the Privacy and Electronic Communications (EC Directive) Regulations 2003 make similar provision applicable to providers of public electronic communications services.

Although there are similarities between these provisions and those in the Bill, the provisions are distinct. They have different purposes, and would largely apply to different types of incidents.

In circumstances where a particular incident constituted both a security compromise and a personal data breach, I consider that the provider could include any information it is required to give to users by Ofcom with any communication required by the UK GDPR. We would also expect Ofcom to cooperate with the ICO in any associated investigation. Ofcom already collaborates with the ICO across their respective remits, drawing on existing frameworks including a memorandum of understanding.

Ofcom's information gathering powers

In the debate on amendment 13, I agreed to provide detail in writing on how Ofcom's information gathering powers could enable it to require information on the diversity of suppliers within a provider's supply chain.

Ofcom's information gathering powers under section 135 of the Communications Act 2003 enable it to require communications providers to provide it with "*all such information as they consider necessary for the purpose of carrying out their functions"* under (inter alia) Chapter 1 of Part 2 of the Communication Act 2003 (in which Ofcom's security-related functions are situated).

In the debate I also drew attention to the amendments made to section 135 by clause 12, which would specify that Ofcom may require "*information concerning future developments of a public electronic communications network or public electronic communications service that could have an impact on the security of the network or service".*

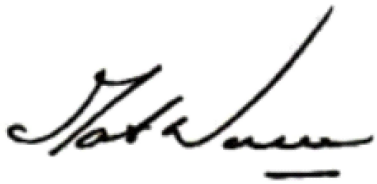
Ofcom could therefore require information relating to the diversity of suppliers within a provider's supply chain if it considered this to be necessary to carry out its functions, such as to assess whether a provider was complying with its security duties by taking appropriate measures to reduce the risk of security compromises.

As mentioned above, I would also draw your attention to clause 23 of the Bill, which confers a new power on the Secretary of State to require information from providers for the purpose of exercising his functions relating to designated vendor directions. That power enables information to be required about the use, or proposed use, of goods, services or facilities supplied, provided or made available by particular persons, and could be used to explore whether a provider or providers risked becoming overdependent on a particular supplier in a way that created a risk to national security.

Therefore, this bill does already contain a mechanism to collect information related to the diversity of a provider's supply chain.

I hope the details I have set out in this letter go some way to clarifying the concerns you and other members of the Committee raised during the scrutiny session, and I look forward to progressing with this important piece of legislation.

I am copying this letter to the Chair and to the other members of the Committee, and will ensure a copy is placed in the House Library.



Matt Warman MP
Minister for Digital Infrastructure