ISPAUK

Cyber Security and Resilience Bill
ISPA Public Bill Committee Response

Background

1. The Internet Services Providers' Association (ISPA) welcomes the introduction of the Cyber Security and Resilience Bill (CSR) and is pleased to be submitting evidence to the Public Bill Committee. ISPA represents 150 organisations that build the infrastructure and connect consumers and businesses to the internet. Given members' critical role, cybersecurity and resilience has long been a priority for the sector, through investment, design, regulation, and best practice.

Telecoms sector prioritises cyber security

2. The telecoms sector is subject to a range of different cyber regulations. The main industry-specific legislation, the Communications Act 2003 as amended by the Telecoms Security Act (TSA), means the sector is more highly regulated than any other sector for cybersecurity. The TSA and associated regulations came into force in 2021 and at its heart consists of over 250 specific technical measures that have to be implemented, alongside specific directions around the use of high-risk vendors by the regulator, Ofcom. A proportionate tiered approach is undertaken, with government given powers to bring specific organisations into scope, alongside specific directions around the use of high-risk vendors. These measures were reviewed and consulted on last year ahead of final updates being confirmed by mid-2026.

3. Ofcom continues to use its powers under Section 105 of the Communications Act for incident reporting. The Privacy and Electronic Communications Regulations (PECR) applies to providers of communication services and the sector has long worked with the authorities under investigatory powers legislation. Furthermore, the original NIS regulations brought into scope services such as internet exchanges and DNS providers.

Scope

4. Having set out the mature set of requirements placed on members, we welcome the fact that the Bill explicitly says it will not apply to Public Electronic Communications Networks and Services (PECN and PECS). However, several ISPA members provide managed services alongside being a PECN or PECS.

5. We are concerned about the risk of duplication and lack of consistency. Having to deal with multiple sets of regulators and legislation, would be overly burdensome. Further it would be disproportionate to adopt different security measures and heavy handed regulatory oversight regimes which all aim to achieve the same security outcomes. We also question

what would happen if a PECN/S were designated a critical supplier by the regulator at a later date under the CSR Bill.

6. Many providers captured by the CSR Bill framework will already be regulated under the TSA, or subject to NIS2 in the EU, for different arms of their business and thus the same entity will face overlapping security obligations and reporting.

7. For those at risk of 'double-regulation' we recommend a proportionate approach that takes account of the practical impact, avoids creating a parallel framework, emphasising consistency, reference to international standards, and mutual recognition of equivalent compliance efforts. If one of our members is regulated by Ofcom as PECN/S but also reports to the ICO for activities undertaken as an MSP, there must be a clear mechanism to resolve any conflict between the two.

Recommendation 1: The Committee should ask government how they intend to deal with regulatory duplication in practice, including through streamlined incidence reporting, beyond a simple coordination duty on regulators

8. Cyber resilience is a cross-border issue and involves multinational organisations and international regulations and standards. These standards should be acknowledged, or at least referenced, for compliance purposes and mutual recognition. We strongly urge the Government look at any framework and/or Code of Practice to existing international standards such as NIST, ISO and the EU's NIS2 Implementing Act which applies to MSPs in the EU, so as to facilitate interoperability of the frameworks and reduce burden for regulated entities.

9. The creation of cybersecurity certification schemes allowing a single certificate to demonstrate compliance across multiple pieces of horizontal and sector-specific legislation would simplify regulatory obligations for entities subject to multiple sets of requirements and help reduce burden and ensure interoperability of frameworks around the world. It is important to ensure that the Code of Practice should function solely as a set of useful recommendations to support each stakeholders specific circumstances in light of their own risk assessments.

10. Avoiding regulatory duplication is especially critical in light of the government's central commitment to reduce the annual administrative burden of regulation on businesses by 25% by the end of this Parliament[1].

[1] https://www.gov.uk/government/publications/a-new-approach-to-ensure-regulators-and-regulation-support-growth/regulation-action-plan-progress-update-and-next-steps

11. We also welcome the fact that security requirements will move deeper into the supply chain, ensuring vital yet often less understood parts of the internet ecosystem are brought into scope.

Reporting

12. We are supportive of the changes to reporting requirements, with incidents needing to be reported in an early and later intervals. However, we note that the new regime maintains the status quo of requiring incident reporting across different sectoral regulators. DSIT should consider streamlining its approach and consider whether it would be effective and efficient for this to go through one single authority. This single, more centralised approach for reporting is used elsewhere, including in Australia and the European Commission's Proposal for a revised Cybersecurity Act includes a single entry-point for incident reporting[2]. It reduces complexity and the risk of duplication, particularly for SMEs and where there may be duplication across regulations. Automation could also be added so that a singular notification is sent to all relevant regulators, and could ensure that any follow ups are handled centrally. Given the short timeframes and high pressure scenarios, we urge the Government to make incident reporting simple for industry.

Recommendation 2: Government should explain why it is not moving towards a more streamlined single reporting function

13. We believe that the adoption of clearer and objective criteria for incident reporting thresholds would ensure consistent and harmonised reporting and prevent regulatory bodies from being overwhelmed by less significant reports, enabling them to concentrate their resources on security incidents that are genuinely significant. Furthermore, the requirement for a regulated entity to issue customer notifications regarding incidents should be confined to scenarios where those customers are directly affected and possess the capability to undertake mitigating measures, in accordance with established best practices. For example, the EU's NIS2 Directive requires customers to be notified "where appropriate" (Art 23(2) of the NIS2 Directive).

Recommendation 3: Government should set out clear objective criteria for incident reporting thresholds and adjust the requirement to notify customers only in relevant situations.

14. Secretary of State's powers

15. The Bill will give the DSIT Secretary of State significant new powers to bring operators of essential services into scope, including MSPs that do not fall within the existing thresholds. While we understand this approach and there are some safeguards built in, the Committee should insist on these safeguards being followed and ensure Parliament is able to adequately scrutinise the SoS' decisions.

[2] https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-eu-cybersecurity-act

16. Given lots of detail will be in the secondary legislation and guidance, it makes it very hard to scrutinise the overall measures and impact of the Bill. It will be important that there is a process that allows for full parliamentary scrutiny once the Bill has passed and industry and others can contribute to this process.

Recommendation 4:Government should set out a clear process and timetable for further scrutiny for implementation once the Bill has become law

Role of regulators

17. From members' experience with the TSA and the accompanying Code of Practice, the Committee should question whether regulators are pursuing a targeted and effective approach to monitoring and enforcing cyber regulation.

18. Ofcom has used its regulatory oversight powers under the TSA to request a large volume of information via statutory information requests. These require significant resources to complete and can distract from the implementation of compliance improvements. Moreover, this has largely been a one-way process, with little communication back on any learnings, and so it is unclear what value this is having. In light of this, we would caution against an oversight model that mirrors a strict TSA-style rolling information requests, given the burdens they impose and the risk of diverting resources from operational security work. More broadly, there is a well documented skills gap in cyber and these new requirements are only likely to exacerbate the situation.

Recommendation 5: Parliament to review more closely whether regulators have the necessary resources and are using them effectively

Consultation

19. We acknowledge the necessity for the framework to remain agile to address new threats; however, strong collaboration and consultation with industry are required when developing secondary legislation. Government and the regulatory authorities must ensure that they provide sufficient time for meaningful consultation with industry. Such consultation should consider not only the substance but also the practical implementation of the framework.

Holistic approach

20. As the UK economy and essential services become increasingly digitalized, the cybersecurity risk landscape has expanded exponentially. The rapid adoption of new technologies has created more entry points for cyber threat actors, this deep digital interdependence means that a single vulnerability in a third-party provider or a supply chain partner can now have a cascading effect across entire industrial sectors. Last year's

high profile attacks crippled key organisations and industries for periods, with huge and large impacts on local economies and supply chains.

21. We started our submission by outlining the high level of regulation and obligations placed on our members. It is important that other sectors and government itself are also subject to a proportionate focus and approach. While this single piece of legislation alone cannot solve the cyber challenge and government has a number of other priorities in this space - guidance, awareness raising, codes of practice, skills, and more - it is vital Parliament uses this legislation to improve cybersecurity and resilience.