techUK.org | @techUK

techUK Briefing on the Cyber Security and Resilience (Network and Information Systems) Bill

This briefing outlines techUK's position on the Cyber Security & Resilience (Network & Information Systems) Bill ('the CSR Bill').

High-level response

techUK welcomes the intent of the CSR Bill which signals the government's ambition to modernise and future-proof the UK's cyber laws while fostering the resilience that will underpin our economic growth; however, our members have some concerns and recommendations.

As currently drafted, the Bill leaves substantial detail to secondary legislation and guidance. These factors will ultimately determine the proportionality, clarity, operability and effectiveness of the regulation for organisations falling in scope, as well as the scope itself. Indeed, as is, **industry requires greater legal certainty to understand duties on entities in scope and what is required to meet them**. Therefore, **the Bill must provide safeguards/a framework around the ability to update criteria that will be set out further in the secondary processes to ensure there are appropriate checks and balances in place within the primary legislation.**

Government must undertake meaningful and mandatory consultation on the secondary legislation and guidance to ensure that the measures are fit for purpose and practicably implementable. Given that the consultation will include a significant number of elements for review, **we would urge government to ensure an appropriate length of time is allowed for the process. We would also encourage government to consider the timing of the consultation period:** the current indication is that it will take place in the 'summer of 2026' but we would advocate for this to be brought forward**.**

techUK's other key asks are as follows:

- The expectations on regulated entities must be clarified to help ensure there is consistency, transparency and accountability across essential services.
- Robust oversight and mandatory consultation should be required on the development of the Code of Practice and regulatory guidance.
- More clarity is needed on the information sharing/gathering requirements.
- Government should work closely with industry on implementing legislation/guidance around when the Secretary of State's powers to issue directions to regulated entities would be used and how the process would work and when it would be allowed.
- Additional support should be given to industry to bear the cost of regime compliance.

You can read more detail on our members' views on the CSR Bill below. If you would like to arrange a meeting, please contact Jill Broom at jill.broom@techuk.org or Alice Campbell at alice.campbell@techuk.org.

February 2026

Key specific concerns

1. The potential for significant burden on regulated entities

Scope and definitions
Further detail is necessary to remove any ambiguity and to help businesses implement the right measures to comply with the legislation, and to reduce unnecessary burden and cost. Because much of the detail is expected in the secondary legislation, this makes it difficult to properly scrutinise the Bill. techUK would encourage a sensible, practical, proportionate and effective approach to the regulations; and we would caution the government against leaving the definitions of key terms unclear. For example:

- **Confusion between a regulated service and the company:** It is unclear whether, if a supplier is identified as being within scope, if this is at an organisational level, or just in the context of the services being provided. Indeed, the legislation refers to service providers in the main categories and places burdens and legal liabilities on the whole organisation (fines at up to 4% of global revenue) and there is conflation of the legal entity (the 'person') with the service. This creates significant confusion and/or issues for companies with multiple services in different categories.

- **The definition of Managed Service Providers (MSPs) remains unclear:** This is still too broad and continues to cause confusion as it is likely to encompass virtually any IT-based service. A clearer definition would help to distinguish between core managed IT services (e.g. IT outsourcing SaaS, cloud or IT infrastructure provision/IaaS) versus general product support or hardware services that utilise IT but are not managed IT services themselves. (Please note that there is a carve out for SMEs, but they could still find themselves being designated a critical supplier.)

- **The criteria for designating critical suppliers remains unclear:** Without clear and detailed (and risk-based) public criteria on how the regulator will identify and designate specific high-impact suppliers as 'designated critical suppliers', there is a risk of arbitrary and/or inconsistent application which would ultimately undermine confidence in the regulation. This is evident when a PECN/S will not be regulated as an MSP as they already fall into scope of the Telecommunications (Security) Act (TSA), but they could still be designated as a 'critical supplier'.

  There is also a risk that regulators would take different approaches to this power: some could take a heavy-handed approach, potentially stifling innovation and flexibility in the technology and cyber security sectors. Furthermore, organisations should be critical to the whole ecosystem (i.e. systemic), and not just a single OES and the language in the Bill should be tighter in this regard. A critical service provider would imply that without that service provider, the customer organisation would no longer be able to operate. This should not be confused with a provider of a service which *supports* a critical function but doesn't *provide* that critical function. For example, cyber is a critical function for a customer, but if the provider's software were to fail, it doesn't take down the customer's network or systems nor does it guarantee that there would be a breach on the customer's network.

There should be a default expectation of reasonable expectation of customer due diligence and risk mitigation avoiding any need for single issue designation and focusing only on systemic issues.

Suppliers need to understand the criteria that would lead to being designated critical, so that they can pre-plan accordingly, or choose to take a course of action that would result in them not having critical designation.

Where a regulated entity is providing the same service to various critical sectors, there should be a single lead regulator ensuring harmonisation of requirements across all regulators – not only the Operators of Essential Services/Critical National Infrastructure regulators but also Her Majesty's Treasury/Critical Third Party Regime and the Information Commissioner's Office. Exposure of up to 14 different regulators for the same service under a single Bill is not acceptable.

Furthermore, concerns have been raised by some members about the critical supplier designation duplicating the TSA**.** Government has indicated that TSA-regulated connectivity services are unlikely to be designated, but explicit assurance, through legislation or statutory guidance, is needed to confirm that TSA-regulated services and their suppliers will not be subject to critical supplier designation, ensuring clarity and proportionality.

Streamlined, risk-based Incident Reporting

- **Simplify the reporting process:** Government has said that it is seeking to minimise the burden on regulated entities. Given the interactions between the NIS Regulations 2018 and other domestic legislation such as the Telecommunications (Security) Act 2021 and the UK Critical Third Parties regime, we continue to ask for harmonisation and streamlining where possible. This should include implementing a single, centralised incident reporting platform. Establishing a unified portal for incident reporting – rather than having multiple regulators independently contact the reporting entity (or regulated entities have to report the same incident to multiple regulators) – would reduce administrative burden and ensure consistent, accurate information is shared with all necessary authorities. Importantly, such a platform must be secure to avoid introducing new security risks.

- **Better clarify what constitutes an actual, or suspected, cyber incident that needs to be reported:** The Bill expands the current definition of an incident in the NIS Regulations to capture incidents that are *capable of* having a significant impact on the provision of the essential or digital service. The term 'capable of' is highly ambiguous and open to interpretation – technically any phishing email is 'capable of' having a significant impact if the organisation lacks adequate detection or response capabilities. This will lead to over-reporting of low-level incidents and potentially overwhelm regulators, thereby distracting attention from genuinely significant threats. A clearer, more rigorous definition should consider and set thresholds for: the level of access obtained, the volume of access obtained, business criticality of systems affected; the sensitivity of information as it relates to business processes or digital infrastructure and the impact of the misuse; and service outage incidents.

- **With regard to the timings of the notification of incidents** [14(e) sub paragraph 5 in the CSR Bill text, greater clarity is required around the phrasing 'beginning with *that time'* in the following to understand if this would mean the second notification is required 72 hours from the point of the first notification, or 72 hours from the point at which the regulated entity is first aware of the incident: *'[the notifications required must be given by]…in the case of an initial notification, before the end of the period of 24 hours beginning with the time at which the RMSP is first aware that an RMSP incident has occurred or is occurring, and in the case of a full notification, before the end of the period of 72 hours beginning with that time'.*

- Further **detail will be required on when incident information needs to be shared with customers**. This should only be necessary when customers are directly impacted and capable of taking action to mitigate any risk. This is for example the approach under the EU's NIS2 which says customers should be notified 'where appropriate' and or 'where applicable' (Art. 23(2) of the NIS2 Directive). Consideration will also need to be made regarding any unintended consequences which could set off an accidental 'chain of law' around other reporting obligations. This needs to be thought through to ensure entities can manage within the bounds of their *cyber security* obligations.

- There is a further opportunity with incident reports to **improve understanding of the impact of end-of-life technology on cyber resilience**, by requiring reports to include details of known vulnerabilities being exploited or unpatchable technology being the root cause.

- Finally, **the sequencing of, and alignment with, other potential regulation will be important.** For example, government's ransomware proposals – which include incident reporting requirements – are expected to be introduced via a different legislative vehicle to the CSR Bill and government must be careful not to add additional layers of confusion, or user journeys into an already complex landscape.

A consistent approach across the regulators

More broadly, a coordinated and consistent approach across the regulators will be vital and we would urge the government to maintain a close relationship with the regulators to avoid a regime that makes it overly complicated for doing business in the UK, or poses barriers to entry for SMEs or new entrants that allow the sectors to keep pace with innovation. Coordination and a consistent approach to interpretation of the regulations across the regulators will be instrumental in helping to reduce complexity, allow organisations to focus on dealing with the cyber incident at hand and help to increase understanding of the risk.

Greater legal certainty

Given the potentially broad and subjective scope on who might be in scope and the subjective nature of the overall commitment – signalled by language such as 'appropriate and proportionate measures' … 'having regard to the state of the art'… 'ensure a level of security of network and information systems appropriate to the risk posed' – there is very little legal certainty to balance the significant legal liability (fines and also regulatory investigative powers and powers of direction).

If the regulation were tightly defined to major digital suppliers, it would be entirely appropriate to have a *presumption of conformity* against the international standards (and therefore access to accredited certification where appropriate). As is, the required commitments are rather too open ended and could be excessive for many organisations now in scope. However, there should be an easy pathway from whatever is required to the international standards to support trade and growth agendas and avoid issues with technical barriers to trade.

Greater certainty will provide clarity to industry and help organisations to determine whether obligations apply, as well as help regulators to take consistent approaches. It will also avoid significant work on clarifying the role of regulatory intervention.

Ask: The expectations on regulated entities must be clarified to help ensure there is consistency, transparency and accountability across essential services.

2. To ensure a future-proofed regime, government must have a mechanism to consult, govern, monitor and update security governance processes as technology evolves

techUK welcome's the CSR Bill's overarching objective of raising the security and resilience of the UK's infrastructure, therefore, members are keen to engage with government to ensure that the Code of Practice and regulatory guidance issued to the regulators are workable, proportionate to a fast-evolving cyber landscape and clearly aligned with the intended outcomes of the Bill. As drafted, the requirement for the Secretary of State to consult 'such persons as the Secretary of State considers appropriate' is too vague and risks inconsistent or insufficient engagement with the affected sectors.

To ensure the regime is agile, achieves proper oversight and avoids unintended consequences, government should:

- engage with industry before issuing any Code of Practice to consider the effectiveness and impact of the Code;
- prepare an impact assessment for regulated entities;
- introduce a review mechanism to ensure the Code remains effective and proportionate to evolving threats and evolutions in defences; and
- establish a clear referencing policy for standards.

Lessons should be learned from the implementation of the Telecommunications Security Act, Electronic Security Communications (Security) Regulations and the TSA Code of

Practice, including (for example) the need to evolve the Cyber Assessment Framework more dynamically than current legislation would allow.

Ask: Robust oversight and mandatory consultation should be required on the development of the Code of Practice and regulatory guidance.

3. Sharing sensitive information has the potential to put regulated entities at risk

The CSR Bill includes strengthened information sharing provisions, with the intention to improve the flow of information related to the NIS regime, creating new information sharing gateways and providing greater clarity on what information regulators can share or receive, and with or from whom, to support the delivery of NIS functions while minimising burdens on businesses. However, industry has some concerns about how this will work in practice.

Different regulators could potentially come to organisations that are deemed critical asking for different types, and quantities, of information which will be very resource intensive – indeed, it is not yet clear what class of information will have to be provided. Further, more detail is needed on what the regulators will do with this information, including how it will be shared, protected, stored and accessed. Clarity is also required on which information sharing tools will be used, when the current information sharing arrangement (CISP) was decommissioned in November 2025. The potential sharing of very sensitive information (from a client data privacy, security and/or commercial point of view) can put organisations further at risk.

Government will have to ensure that regulators share responsibility for protecting sensitive data and that information-sharing processes are coherent, proportionate and secure.

Furthermore, there could be a reduction in burden by relieving organisations from having to share information which (a) isn't immediately retrievable in the course of business; or (b) poses a security risk to that organisation or its customers; or (c) would place that organisation in breach of any of its contractual obligations to its customers.

Ask: More clarity is needed on the information sharing/gathering requirements.

4. More detail required on the safeguards around the new powers of direction

The CSR Bill will grant new powers to the Secretary of State to issue a direction to regulators and regulated entities to take necessary and proportionate action to respond to threats to the UK's national security. This will include enhanced monitoring and isolation of high-risk systems. We fully appreciate that these provisions are trying to address the dynamic nature of the cyber security ecosystem, but we would welcome further detail. While we also appreciate that the government's intention will be to use these powers in cases of national security, we believe that reliance on national security is insufficient – there are many documented cases of abuse of that largely self-defined term – and in the current volatile geopolitical environment, industry would welcome objective language, clearer safeguards, greater transparency, and robust oversight mechanisms. We previously recommended secondary legislation be used here, with full consultation under the positive assent procedure.

Ask: Government should work closely with industry on implementing legislation/guidance around when the Secretary of State's powers to issue directions to regulated entities would be used and how the process would work.

5. Compliance will require significant investment

New regulatory regimes incur significant compliance and implementation costs for businesses, especially if imposed in the middle of existing long-term contracts. techUK members have concerns that the publication of the Bill's impact assessment (IA) occurred without consultation, therefore, more clarity is required in key areas such as the cost of information sharing/gathering, which could be significant for organisations. Furthermore, industry would welcome more information on the following points:

- What financial or practical support will government offer to help businesses meet new security requirements?
- Will incentives be considered for regulated businesses to ensure they are compliant with the new measures?
- How will the government avoid conflicting incentives and disincentives – for example, exposure to regulators and fines due to incident reporting?
- How will those areas that are not clear in scope, but require proactive registration by businesses, by handled?

Ask: Additional support should be given to industry to bear the cost of regime compliance.

Additional points for consideration

1. techUK welcomes the addition of **data centres** under the NIS Regulation. However, there is a significant lack of detail which must be clarified through secondary legislation and robust and meaningful consultation with this sector. This is particularly important, because data centres were not consulted previously. Furthermore, additional clarity is needed on the scope as some data centres risk falling between the scope of "data centre" and "managed service provider", increasing uncertainty and risk of duplication for reporting requirements.
2. The majority of **the public sector remains out of scope** of the Bill, and yet departments such as Department for Work and Pensions, HMRC and Local Authorities all offer critical services which vulnerable people in society rely on. Reports earlier in 2025 by the National Audit Office and Public Accounts Committee have highlighted significant gaps in the government's own cyber resilience, underscoring the need for the public sector to enhance its cyber resilience. In keeping with the UK Government's long-term ambition to be an exemplar in cyber

security best practice, expanding the scope of the CSR Bill to include government would ensure that it leads by example and has credibility when talking to business and society about the need for good cyber security. Furthermore, the public sector is in scope of the EU's NIS2 Directive. While we appreciate that government departments are required to follow the Cyber Assessment Framework (CAF) and that the GovAssure scheme is in place, many of our members believe that exempting the public sector risks impeding the secure delivery of the UK Government's priorities for public service digital transformation.

3. It is important to note that sectors which have been the victim of particularly disruptive cyber-attacks across the UK economy this year are not directly in scope of the CSR Bill, including retail and manufacturing. The Bill should not, therefore, be viewed as a 'silver bullet' and **further measures to boost economy-wide cyber resilience must continue to be progressed and implemented**.
4. The CSR Bill presents **an opportunity to reinforce the message that cyber security and resilience is a fundamental board-level responsibility** and treated with the same importance as financial, operational and legal risk. This could be achieved through mandating that company boards are accountable for their organisation's cyber resilience and, as part of this, actively engage in understanding, assessing and mitigating their cyber risk.
5. **Some further clarity on penalties related to incidents is required:** While the CSR Bill does state that the 'impact of the failure in respect of which the penalty is imposed' should be taken into account when regulators issue penalties to regulated entities, members would find it helpful to understand more about what the framework and/or guidance to determine this will look like.
6. **It is important to have formal alignment on regulation between the CSR Bill and the Critical Third Parties regime**, and between regulated requirements and general procurement requirements. If there are no specific enhanced requirements, being regulated should be enough for the private sector and thus Cyber Essentials+ should not be a requirement.
7. **A clear and unambiguous Telecommunications (Security) Act carve-out must be maintained.** We support the Bill's exclusion of PECN and PECS, but an explicit carve-out is needed to ensure TSA-regulated connectivity services are not inadvertently captured through adjacent or ancillary activities. Services already comprehensively regulated under TSA must not face dual obligations.

Contact details

For more information, or to arrange a meeting, please contact Jill Broom at jill.broom@techuk.org or Alice Campbell at alice.campbell@techuk.org.

February 2026

UK Cyber Security and Resilience Bill

techUK Proposed Amendments for improving legal certainty for both suppliers and regulators

Explanatory note

This paper proposes key amendments to improve legal certainty, thus reducing the costs and burdens of this new legislation for both suppliers and regulators. The proposal uses existing regulatory models supporting compliance and introduces a duty to consult on the key areas not covered by secondary legislation, improving the overall governance of the regime. This is a minimum level of change necessary to deliver a balance between the extremely high level of regulatory intervention and fines with a limited level of legal certainty to operate and invest in the UK.

The first amendment (which covers RDSPs, MSPs and DCSs – who all have the same overriding requirement) introduces the ability for the government to designate national or international standards (in part or in full) as a means to support regulatory compliance. The approach is structured as per https://www.gov.uk/guidance/designated-standards. This is the normal method for market regulations in areas such as product (meaning goods and services) safety, for example, medical devices as used in the UK and in the EU single market since 1985 (the 'new approach' or 'new legislative framework').

A designated standard grants a **presumption of conformity** when a relevant product that conforms to the designated standard is used by the regulated entity. However, this presumption is a '**rebuttable assumption'**, meaning it can be challenged and overturned by the regulator if evidence proves otherwise. The supplier must have full documentation of the certification process available to the regulator on demand so due diligence is evident.

This structure creates a reliable and trusted legal framework granting suppliers a clear approved route to compliance and creating a baseline for regulatory assessment and intervention. This proven approach reduces the cost of compliance both to suppliers and regulators whilst achieving very high outcomes and the designated standard can be updated much faster than regulation as threats and technology changes.

It also ensures that key issues are handled automatically by the governance of the de jure standards body, including consultations compatible with World Trade Organisation requirements on potential Technical Barriers to Trade, intellectual property rights, amendments and updates.

A particular focus should be on ISO/IEC 27001 in due course, as there is an existing reference to international standards in the Bill in section 12(2)(c)(v). Designating an ISO/IEC standard would support inward investment and export growth by aligning with the only widely accepted global standard that uses a risk-based approach with controls across the people, process and technology areas fully aligned with the approach in the proposed Bill. A de jure international standard is, by definition, the consensus on best practice. In this case ISO/IEC 27001 is based on BSI's earlier work (originally BSI 7799 from 1995) and the standard has been written into regulation in some European countries, notably Belgium, granting a presumption of compliance for the EU NIS2.

This also means companies and regulators can, where appropriate, avail themselves of accredited certification. The ISO/IEC 27001 is one of very few standards where there is a standardised conformity process with our National Accreditation Service and the International Accreditation Services to ensure a competitive market in third-party certification all upheld to the same high equivalent certification requirement. This ensures that all accredited certifications are equivalent.

Importantly, this formulation does not obligate suppliers to use the designated standards and allows the regulators to offer guidance on both use of the designated standards and alternatives and the level of proof of compliance they would require for any approach without standardised certification. However, it does allow for companies outside the scope of the Bill to voluntarily certify to the standard, avoiding unnecessary market stratification and creating a route to wider resilience and good cyber practice across the whole economy.

Hence, in order to ensure the codes and guidance are effective and enforceable they should be subject to the normal rules of good governance including necessary and sufficient consultation. Secondary legislation is already covered by this requirement, but the key important and high-impact codes and guidance are not explicitly covered with respect to the entities regulated unlike other regulations in this space like the Telecommunications (Security) Act 2021.

<u>The Amendments</u>

Improving Legal Certainty via Designated standards

To be added after 14B for RMSPs, after 12 for RDSPs and after 3ZC for DCS

(1) A service provided by a [RMSP/RDSP/DCS] that is in conformity with a designated standard shall be presumed to be in conformity with this regulation with regard to the obligations [in 14B (2)/ in 12(2)/as set out by the competent authority] .

(2) A standard may be designated, in full or with restrictions, in reference to (4);

a. ***By the Secretary of State; or***

b. ***By the Information Commission (or other relevant designated competent authority) as part of statutory guidance provided to regulated entities***

Improving the governance requirements of the codes and guidance

NB existing text in italics – new text in bold.

Guidance

*(3ZB , 4(B)) When preparing guidance under paragraph [(3)(b) / (4)(b) , the (Information Commission/designated competent authority) must have regard to any relevant code which is in force, so far as the code appears to the Information Commission to be relevant to persons regulated by it, with a view to ensuring that the guidance is consistent with the code**. The (Information Commission/designated competent authority) must consult on such guidance open to all companies offering services in scope of said guidance.***

Codes

36 Code of practice

*(3) Before preparing or revising a code under this section, the Secretary of State must consult such persons as the Secretary of State considers appropriate**, including at a minimum a consultation open to all companies offering services under the purview of regulators addressed by the code.***

UK Cyber Security and Resilience Bill
techUK Proposed Amendment to Incident Reporting Requirements

Explanatory note

The Cyber Security & Resilience Bill (CSRB) currently proposes a reporting threshold for incidents "likely to have a significant impact."

This definition is excessively broad and fails to recognise the practical consequences for regulated entities and the regulator(s). The current formulation would lead to reports of non-material events (e.g. phishing emails) from all regulated entities. This level of reporting would create a cacophony of “noise" for regulators and divert valuable resources away from truly systemic threats.

techUK proposes an amendment, supported by the majority of our members (some members have pushed for an even tighter definition), that allows regulated entities to have greater certainty as to which incidents must be reported to the regulator.

This refined threshold is based on measurable disruption and material business impact to ensure a proportionate and effective regime. The amendment allows government and parliament, via secondary legislation, to set some aspects of the threshold.

This revised language introduces:

- Measurable Metrics: The focus shifts to *non-trivial interruption* and *material portion* of customers, tying the reporting requirement to concrete business and/or operational consequences that affect a significant number of users or critical entities.
- Imminence and High Probability: Replacing the vague “likely” with “highly likely” and “imminent and measurable high risk” requires a higher degree of certainty, compelling the regulated entity to apply professional judgement and technical analysis rather than reporting all ‘potential’ threats.
- Focus on Security Breach Indicators: The inclusion of unauthorised control or compromise of core security controls ensures that successful pre-positioning and other stealth attacks are reported, but only where the breach has reached a defined level of security failure and subsequent risk.

This approach aligns with the need to capture a broader range of damaging attacks like ransomware, while ensuring that the regulator's limited resources are focused on incidents that represent a genuine systemic risk to the UK’s economy or the day-to-day functioning of society.

The Amendment

Proposed amendment for incident reporting threshold

The following text is proposed to refine the criteria for a "significant incident" that triggers the 24-hour initial notification and 72-hour full report obligations:

"An incident affecting the operation or security of network or information systems relied on to provide a regulated service shall be deemed to have, or be likely to have, a significant impact, and thus be reportable, if it meets ***any*** *of the following criteria:*

1. ***Causes a Material Service Disruption:***
The incident has resulted in or, based on a reasonable and objective assessment, is highly likely to result in, the non-trivial interruption or degradation of the core functionality of the regulated service for a duration that exceeds a predefined threshold ('to be defined in secondary legislation based on sector-specific service level agreements// X amount of hours), directly impacting a material portion of the customer base or a designated critical customer.

2. ***Results in an Unauthorised System Control, Adversarial Compromise or Data Exfiltration:***
The incident involves the unauthorised, persistent or escalated access or control of the regulated entity's core network and information systems, or the successful exfiltration or irreversible destruction of sensitive customer data or core operational data, even in the absence of full service disruption. This does not include adversarial cyber activities that do not result in a material business impact or high risk of a service disruption, including but not limited to actions like routine phishing, scanning, or probing of networks and systems.

3. ***Compromises Core Security Controls***
The incident has demonstrably bypassed, disabled, or rendered ineffective one or more core security controls (e.g., firewall, advanced threat prevention, identity and access management systems, zero trust mechanisms) relied upon by the regulated entity to provide the service, and this compromise exposes the organisation's environment to an imminent and measurable high risk of material business impact."