techUK

techUK.org | @techUK

Data Infrastructure, Security, & Resilience Policy Team
Data Directorate
Department for Science, Innovation, and Technology
100 Parliament Street
London
SW1A 2BQ
United Kingdom

Response to the Department for Science, Innovation, and Technology Consultation

Protecting and enhancing the security and resilience of UK data infrastructure

22 February 2024

techUK welcomes the opportunity to respond to the Government's Department for Science, Innovation and Technology's (DSIT) Consultation on *Protecting and enhancing the security and resilience of UK data infrastructure*.

We would also like to thank the Department for its significant engagement throughout the Call for Views and ahead of the current open consultation, including industry roundtables, visits to industry data centre operator premises as well as wider engagement with techUK's Data Centres Council.

We welcome the Government's recognition of the value and crucial role the data centre sector plays in the UK's modern digital economy and note its intention to continue to build the right business environment that encourages investment in the sector allowing for its growth and continued innovation, and ensuring capacity can meet the UK's ambitions for economic growth, scientific progress and safe development of artificial intelligence and other new technologies.

We provide an overview of views on the consultation proposals as well as answering specific consultation questions further below.

Summary and recommendations

We understand the rationale to improve and assure the security and resilience of UK data infrastructure.

We do note, despite continuous interactions with DSIT and the data directorate, the scope of the consultation seems to draw no distinction between responsibilities between data centre providers

and application owners (service and platform providers). A full implementation of the proposals could have the following impact on the sector:

- Potential duplication of efforts and compliance to provide data and reporting across interdependent pieces of regulation;
- An unnecessary increase or duplication in regulatory and compliance costs;
- Potential loss of market flexibility and innovation if the regulator were to impose a set of rules which diverged from international norms and established best practice;
- Potential commercial costs in complying with additional controls set by a regulator.

techUK and the majority of our members disagree with the Government's assessment that there is an unaddressed risk borne by the data centres within scope of this consultation.

This consultation covers a wide array of complex issues in a fast-growing and diverse ecosystem. The issues covered range from commercial relationships between data centres and their customers to supply chain security and the interdependency of cyber and physical risks.

The Government has identified some risks in this consultation which we consider to be of too low a threshold to be reported under the current proposals (i.e. vandalism such as graffiti) or where the responsibility would not reside with the data centre operator, but rather with other actors in this complex ecosystem (data centre customers, network operators etc). Many security and supply chain risks associated with the data centre sector under scope are already managed (if not always formally regulated) across the system.

Whilst techUK members understand and support the need to strengthen resilience per the fourth mission of the National Data Strategy (2020), the second pillar of the National Cyber Strategy 2022, the Government Cyber Security Strategy 2022, as well as the more recent Integrated Review Refresh (2023), and the UK Government Resilience Framework (2022), the sector is currently adequately addressing risks.

Government may want to consider a proportionate barrier to entry framework that won't cause issues for SMEs – if that might meet the aims identified with DSIT's risk assessment.

We note that Government refers to internal analysis which has led to this assessment, but failed to provide access to it for industry to be able to review and respond appropriately to this consultation and to the claim that there is an unaddressed risk. We also note that this is common with other current cyber security policy proposals (see further below).

Recommendation: We would recommend that Government reconsider carefully their risk assessment and thresholds. In particular, Government should consider clearer proposals and re-engagement with key stakeholders on:

- **what** should be reported (as many reporting requirements are already covered under other compliance requirements, or contracts);
- **who** should be reporting (whether the reporting responsibilities lie with the sector under scope of this consultation), and
- **why** some incidents should be reported (what the threshold for an incident to be reported should be, what the desired outcome is, and what the regulator will do with that data).

techUK and our members have concerns over the aims of this consultation and its proposed framework.

While techUK and members support the principles of a risk-based framework, and recognise the attempt to capture areas outside of the current Network and Information Systems Regulations 2018 (NIS), mainly part of data infrastructure such as data centres, we have significant concerns about potential overlap, duplication or unnecessary complexity as this activity occurs in parallel to the updates to the NIS in the UK.

Industry's concern is that both the aims of this consultation and the draft UK NIS Updates are to the same end. There is a lack of practical understanding of how both regimes will interact, particularly as there is no legal text yet available for the UK NIS updates, and the potential for burdensome duplication of effort and compliance to provide data and reporting across these two interdependent pieces of regulation (as well as further ones listed below).

techUK would also like to highlight that this is a hugely diverse ecosystem of companies, all with different commercial models, risk profiles and strategies. The potential impacts of this intervention on that eco-system needs to be considered further.

Recommendation:

Therefore, we would recommend that instead of attempting to carve out parts of data centre infrastructure (namely colocation and "co-hosting"), Government should:

- Pause before considering further policy development and conduct a comprehensive review of how the various Government proposals relating to cybersecurity and resilience in digital markets fit together in both scope and legal frameworks. The interdependencies outlined in the section below, and the lack of clarity on most of them, makes it challenging to provide a constructive response and introduces the risk of overlapping requirements, duplication of reporting and compliance costs, and at worst, inconsistent regulations.
- Assess the merits of alignment with the EU's ENISA NIS Directive (EU NIS2), and existing ENISA guidance (which includes cloud computing service providers and data centre service providers). Diverging from International and EU standards with our own UK scheme risks increasing compliance costs for businesses operating internationally and fragments further an already complex cybersecurity environment. The Government should consider whether the proposed new framework for data centres set out in this consultation is merited i.e. whether it adds anything additional that is not already catered for by the proposed updates to the NIS framework at EU and UK level.

techUK and our members agree there could be room for improvement in terms of information sharing with the UK Government and relevant regulators beyond already existing compliance and regulatory frameworks – mainly threat analysis and incident response.

The Public-Private partnership within the UK cyber eco-system is already world-leading, but avenues for further collaboration can only strengthen this further. Whilst there are challenges around diversification post-Brexit, there remain opportunities for the UK to lead on developing and implementing internationally recognised standards, as we have seen in areas such as the PSTI Act.

Industry also sees positively the role of a new Government/industry forum, which could reunite industry, experts, trade association and Government officials from key Government departments

to coordinate responses to broader industry challenges, such as grid power availability, better planning policy, reliability and move to net zero.

Potential Regulatory Overlaps

Our key concerns, further explained below, are in regard to risks of regulatory overlap and potential inconsistencies with customer reporting duties.

We urge DSIT to consider how the proposed framework will align with existing, upcoming and in-draft UK NIS regulations and to take into account any existing standards/certifications that data centre providers are certified and operate to (i.e. ISOs) as best practice frameworks as long as the scope of those certifications/standards take into account security (both physical and of the services) and resilience (Business Continuity).

This requirement is already in most data centre operators' customer contracts, and they are audited annually. Other country/region-specific standards can also be considered based on the territories the operators are located in.

Along these lines, we urge a *de jure* standardisation approach to the UK's CNI programme particularly the Cyber Assessment Framework (CAF) including independence, regular stakeholder engagement, clear maintenance and consultation processes. This also means a best practice approach to WTO TBT obligations, ensuring the CAF is certification ready and accreditation and certification arrangements are compliant with best practice (ISO/IEC 17011 series). Whilst there is a clear role for security agencies like the NCSC in identifying CNI and commenting on standards, the CAF 'standards-like' style approach correctly belongs with a proper standards body like BSI who will also already have the appropriate liaison status with other national and international standards and can bring it into alignment and remove its subjective nature.

Interdependencies – Data and Cyber:

UK NIS Updates and EU NIS2: This consultation occurs within a wider set of resilience and cybersecurity-related consultations with both internal and external dependencies, as well as exploring existing Critical National Infrastructure (CNI) and Operators of Essential Services (OES) powers. We note that although updating UK NIS to include Managed Service Providers (MSPs) and possibly several other clarifications, there is no draft text available nor details for an outcome to conduct an analysis on practical interdependencies and delimitations between the sectors defined to be in scope.

The UK NIS update consultation included expanding reporting requirements beyond business continuity in a way that would conceivably overlap with the reporting regime proposed here for colocation and "co-hosting" - any proposals to bring cloud and MSPs into scope need to be accompanied by clarity from Government on the status of the NIS Updates. techUK understands limited Parliamentary time is delaying these updates to the NIS Directive, perhaps presenting an opportunity for further engagement between Government and industry on these key areas.

It is also the case that most (if not all) the companies affected by NIS Updates in the UK will also be subject to the NIS2 reforms ongoing in the EU. This is a truly global landscape with international

companies operating across territories. Alignment, clarity, and consistency are vital to ensure citizens reap the benefits of ongoing digital transformation.

The technical security measures for digital service providers set out by ENISA (specifically highlighted by the Information Commissioner) include data centre security measures so it is clearly contemplated that physical security of the datacentre is covered as part of the digital service provider's obligations. Equally, NCSC's latest Cyber Assessment Framework has recently been updated to include physical security measures (although note the above concerns on this process).

The burden will likely disproportionally fall on smaller operators, and in that case, they will be dependent on the activities of their customers to establish if they are regulated. This could be complicated as smaller data centre businesses could be measured on a different basis as qualifying compared with the NIS thresholds, and therefore small data centre hosting or providing cloud or managed services falling below the NIS thresholds could still be subject to CNI but not NIS. This also highlights a lack of clarity on the systemic risk due to scale, in which case SMEs can largely be excluded, or risk due to criticality of service in which case SMES must be included, noting however that this is not required if there is clearer consolidated and harmonised procurement advice, especially for public and regulated sector procurements.

We urge DSIT to collaborate further on the future development of UK NIS when the parliamentary timetable allows, as both this and the NIS consultation are looking at the ability to use secondary legislation to amend the scope but have limited or no details on safeguards such as statutory consultation and regulator alignment. We know that DSIT is keenly aware of the need to ensure appropriate alignment across key Government interventions in the cyber domain. It is clear that 2024 will see further consultations and Government responses covering various topics including, Software resilience and security Cyber Governance Code of Practice: and AI Resilience. Industry believes that some clearer mapping and signposting of how these interventions link, overlap and complement each other is essential to produce clear and effective policy.

With regards to the UK Data Protection Act 2018, generally, colocation data centres as legal entities do not process personal data, but a cyber-attack could be targeted to try to access their customer's personal data - *the ICO defines a personal data breach as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.*

For colocation data centres, they do have and process some Customer Data (sensitive, not for public consumption), regarding contracts, reports, Access Control, CCTV amongst other things, but there are already strict controls in place with regards to sharing. However, there is a limitation to what personal data a data centre operator will have access to. For example, they will not have access to, or even knowledge of, what personal data may be stored in the customer equipment housed in the data centre. This would instead be the responsibility of the customers, including in the event of a data breach where a report to the competent authority may be required.

One key issue is that data centre's customer confidentiality must be maintained under any regulatory intervention of this nature.

Additional Interdependencies

In addition to data and cyber regulation, there is also sector specific regulation, in particular financial services regulation and PCI DSS which have requirements for physical and data security that apply directly to data centres.

- **Financial Services: FSMA 23:** The Financial Services and Markets Act introduced new primary legislation on digital services to the finance sector, enabling regulators to create a new regime which brings technology firms under their scope for the very first time. This granted unprecedented powers without full formal consultation. In establishing this regime, regulators have issued the Consultation Paper CP26/23 - Operational resilience: Critical third parties to the UK financial sector. This new regime is under consultation and its scope is yet to be confirmed, however, inevitably it will cover some providers which are covered also by this consultation. The Bank of England has conducted a cost benefit analysis and estimates the annual ongoing compliance costs of approximately £660,000-£930,000 (one-off) and £500,000 (annual on-going) respectively per Critical Third Party (CTP), although members have suggested the total cost may actually be much higher. Duplicating regimes will cost these firms even more for little/no marginal return on resilience to the UK's data infrastructure.

  Furthermore, it is worth noting that, in the EU, DORA is *lex specialis* and supersedes NIS2. Something to be mindful in the current consideration of CTPs, including MSPs and data centres within scope as this overlap and duplication is already causing confusion and regulatory gridlock.

- Other FSMA 23 measures to consider as complementary (at best) or conflicting (at worst) to the regime contemplated by this consultation include the new Digital FMI Sandbox and the amendments to the regulatory perimeter to include digital assets.

- **AI White paper:** The AI Whitepaper advocates for a risk-based approach. A risk-based approach means focussing on the context of use; and that can only be done by the party determining the context Indeed, we have praised the world leading AI white paper for supporting this very principle and it is concerning to see it undermined in multiple consultations simultaneously.

- **Freedom of Information Request:** We are mindful that this may create additional risks based on the proposals of this consultation. Social Engineering, Phishing, Hacking are at an all-time high and becoming ever more elaborate and companies falling foul to this. If date is collected by Government on the industry, this data could fall in the wrong hands through the Freedom of Information, with potential severe consequences. Therefore, there should be explicit assurances that information disclosed as part of any regime should be explicitly exempt from FOIA on security grounds. Regulators are becoming major targets for hostile attackers seeking to carry out reconnaissance and discovery.

We include a glossary of terms used in this response for ease at the end of this document.

techUK's Response to the Consultation Questions

Voluntary measures and industry support structures - *Critical National Infrastructure status*

The UK Government is considering how the data infrastructure sector fits into the Critical National Infrastructure (CNI) framework and whether third-party data centre infrastructure should be determined as a subsector of CNI in its own right due to the increasing reliance on these services by the UK.

While the Government is correct in its assessment that parts of the data centres sector will meet the definition of CNI, it is worth noting that individual operators with sites and contracts which fit the current CNI have sought the designation for those sites. However, this means that designation is entirely dependent on the clients and services in the data centre, which could change overtime, and could make it hard to have a consistent approach across all data centre providers. Furthermore, data centre providers may not know that their facilities would be considered CNI as a result of the services being provided unless they are informed by the tenant providing them.

While techUK recognises that the designation (not a proposal yet) can have advantages such as exemptions from planned power cuts such as in the Government's recent Reasonable Worst-Case Scenario (RWCS), designation also entails additional obligations on reporting. How these obligations would interact with the current proposals is not clarified.

Question 4: *What forms of digital or data-related infrastructure should the Government the Government consider for potential CNI designation?*

techUK understands that this consultation focusses on hosting and co-location data centres, although a number of references are inconsistent with this focus However, even if, as techUK recommends this is restricted to a clear infrastructure definition, these exist in a broader data networks and connectivity ecosystem which is digital or data-related infrastructure, of which, parts such as the telecommunications sector, already have CNI designation. Some of the risks are covered under the Telecommunications (Security) Act 2021. Therefore, duplication and complexity of compliance is a key concern for techUK members. For example, some colocation data centres also provide connectivity within their campuses as between customers.

The risk of data-related services failing can largely be mitigated by following best practice of service design, as mandated by the FCA and is embedded in customer due diligence as they follow their own risk-based approaches normally under ISO/IEC 27000. This includes secure service design, replication and redundancy of service computing between several geographical sites, redundancy of network links, separate regular and secure backups of the data that allows restoration of the service etc. This is the responsibility of the tenant where this is different from the data centre operator.

If standardised best-practice is followed in service design, a catastrophic failure of a data centre site or even an entire data centre operator's sites would not actually impact the availability of the service itself. As a result, there is no obvious part of the data centre infrastructure that intrinsically fits the CNI definition. The parts of the infrastructure that could be relevant only occur when they are entirely and uniquely (i.e. no redundancy exists) linked to the services they serve, which are subject to change and may not be visible to data centre operators.

Furthermore, we note that under CNI the 13 national infrastructure sectors are clearly defined sectors. Data centres as per the scope of this consultation are not a sector, but rather a carve-out made by Government to fill a perceived regulatory gap.

Question 5: *How would you compare the expertise required to appropriately risk manage the colocation data centre sector to other critical sectors, such as Communications?*

The risks to data centre operations at a high-level stem from two areas:

- Risks impacting the physical infrastructure, whose management requires skills in mechanical and electrical engineering, physical security and facilities management;
- Risks impacting the data centre operator's wider business operation and supply chain, including information technology (IT) and operational technology (OT) systems, which require IT skills more aligned to those required in the communication's sector.

Similarities

- Both require understanding high-level threats and vulnerabilities: Both sectors face similar threats like cyberattacks, physical and natural disasters, and power outages. Experts need to identify these threats, analyse their potential impact, and develop mitigation strategies.
- Both rely on multi-disciplinary expertise: Effective risk management involves professionals from various backgrounds like security, engineering, disaster recovery, and compliance, as well as reliance on third-party suppliers.
- Both need strong communication and collaboration: Sharing information and coordinating efforts with different stakeholders within and beyond the sector is crucial for effective response and preparedness.

Differences

- Specificity of technical knowledge: Colocation data centres have unique infrastructure and operational complexities compared to communication networks. Risk managers need deep technical knowledge about power systems, cooling systems, physical security, and specific IT equipment vulnerabilities. This is the same for communications providers in respect of facilities, such as nodes, in which communications equipment is sited and operated.
- Regulatory landscape: Data privacy regulations and compliance requirements for data storage are often stricter than those for network communications. Expertise in navigating these regulations is vital for data centre risk management, but only to the same degree as any other organisation processing data. A colocation operator, for example, will not know what is being stored on customers' infrastructure.
- Business model considerations: While communications providers offer direct services to end-users, colocation data centres primarily serve other businesses. Risk management needs to consider the cascading impact of disruptions on client businesses and their diverse needs.
- Focus on data security: Protecting sensitive data stored or processed in colocation facilities (as previously mentioned, this is very limited) necessitates additional expertise in data security measures like encryption (although in the case of a colocation data centre this responsibility is only on their own networks), physical and logical access control, and

incident response. Depending on the customer mix within a colocation data centre, there may also be critical requirements from customers on physical security of the site and facilities.

Question 6: *Are there particular benefits, opportunities, or risks to CNI designation for the colocation data centre sector that you would wish to draw our attention to?*

Whether or not data centres should be designated as Critical National Infrastructure (CNI) in the UK is a complex question with no easy answer. There are strong arguments to be made on both sides of the issue and considerations for those data centre sites that have Government contracts or host Financial Services as a customer, which will already either fall under CNI or be compliant with other regulations.

The specific benefits, opportunities, and risks will vary depending on how CNI designation is implemented and the level of detail in the regulations. Therefore, techUK and our members urge for a proportionate approach, with support from the Government balancing the extra requirements and restricted to infrastructure not higher-level services or abstraction layers.

Clear communication and collaboration between the Government, industry, and other stakeholders will be crucial to ensure that CNI designation is effective and minimizes negative impacts.

Ongoing monitoring and evaluation of the impact of CNI designation will be necessary to ensure it is achieving its intended objectives without causing undue harm to the data centre sector.

Benefits and opportunities

- **Designating data centres as CNI may formalise the information exchange between Government and the data centres sector**. Collaboration between Government and industry could be strengthened under CNI designation (and this should be considered with an independent intermediary), facilitating information sharing and better-coordinated responses to threats. This could include notifications of the need support, particularly around energy security. An example of this has already been flagged by techUK and members around fuel prioritisation in some circumstances in response to the Government's Reasonable Worst-Case Scenario (RWCS).
- **Data centres are essential to the UK economy and society.** Data Centres house equipment which stores and processes data for a wide range of critical services, including the energy grid, healthcare, finance, and Government. A cyberattack or other disruption to a data centre could have a major impact on these services, if they are not appropriately designed and managed, causing significant economic damage and social disruption. However, individual operators with sites and contracts which fit the current CNI have sought the designation for those sites.
- **Data centres are increasingly potential high-value targets to cyberattacks.** As they become more interconnected and store more sensitive data, they become more attractive targets for attackers. While it is true that the UK Government has a role to play in taking steps to protect these critical assets from cyber threats, it is also worth noting that the sector takes cyber-attacks incredibly seriously and mitigates through several appropriate measures. ISO/IEC 27000 approaches, whether 3rd party certified or not, mean continuous feedback and improvement as data centre scale and threats change. Worth noting that most cyberattacks

focus on the data centre customer and between network segregation and existing mitigations, this remains contained to the customer.

- **Designating data centres as CNI would allow the Government to impose more stringent security and resilience requirements.** CNI designation could trigger increased Government funding and support for cybersecurity initiatives, leading to more robust security measures within data centres. This could benefit the entire sector by raising overall standards and making data centres less vulnerable to attacks.
- **Increased trust and investment**: Public perception of data centre security could improve with CNI designation, potentially attracting more business and investment to the sector. If CNI designation leads to demonstrably improved security standards, without causing a significant rise in cost of supply, it could give UK data centres a competitive edge in the global market.
- **Improved access to talent and resources:** CNI designation might attract skilled security professionals and resources towards the data centre sector, further bolstering its security posture - as long as it is consistent with international standards to avoid fragmenting the skills base.
- **Development of innovative security solutions:** The need to meet stricter security requirements imposed by CNI designation could spur innovation in the data centre sector, leading to the development of new and more effective security solutions.

Risks

It is not clear that designating data centres as CNI would make them more secure. The Government would need to invest significant resources in developing and enforcing new regulations.

- **Discourage investment:** There is a risk that designating data centres as CNI could damage the UK's reputation as a business-friendly environment. This could discourage foreign investment in the data centre industry.
- **Regulatory burden and increased costs**: A blanket CNI designation across the sector could entail significant new regulations and compliance requirements for data centres, leading to increased operational costs and administrative burdens. UK-specific interventions especially aligned with UK security agencies like the NCSC could significantly impact UK reputation overseas and increase costs of supply. Furthermore, increased operational costs may be passed on to customers which may undermine competitiveness and drive colocation owner/operators to prioritise investment in overseas facilities.
- **Stifling of innovation**: Excessive regulation could hinder innovation in the data centre sector, potentially slowing down the adoption of new technologies and business models.
- **Disproportionate impact on smaller players:** Smaller data centres might struggle to cope with the financial and logistical challenges of CNI compliance, potentially putting them at a disadvantage compared to larger operators. At worst, they could exit the market and therefore reduce choice and increase concentration risks.
- **Market impacts:** This could also lead to market distortions, by creating higher barriers to entry to the sector and increasing the overall cost of DC services, including for clients for whose application high level of resilience are less important than cost.

Other voluntary measures and support structures

***Question 7**: What forms of intra-sector and sector-to-government voluntary cooperation would be most useful for the sector?*

The adoption of professional standards, titles, and registration. Professional titles are a mechanism for ensuring competency, while professional standards provide a framework for security measures in practice.

As noted above, there are a material number of complementary or different rules and regimes which are in development or are in force already: intra-regulator/policy-maker communications are vital prior to public engagement and consultation.

***Question 8:** What voluntary cooperation mechanisms, if any, have you experienced in this or other sectors that demonstrate improvement to risk management?*

The establishment of professional standards and adoption of professional titles within various sectors have significantly contributed to improving risk management practices. Defining clear guidelines and benchmarks for competency and performance through the adoption of professional standards help provide a structured framework for organizations to assess and mitigate risks effectively, ensure a consistent level of proficiency among professionals, and foster a culture of accountability and professionalism within the industry.

***Question 9:** Which issues lend themselves to intra-sector cooperation, and on which issues would industry welcome further Government involvement?*

The adoption of professional standards within sectors often lends itself well to intra-sector cooperation, particularly on issues directly related to enhancing industry-wide practices and standards. Matters such as the development of common frameworks for risk assessment, the establishment of ethical guidelines, and the promotion of standardized certification processes are prime examples where intra-sector collaboration can be highly effective.

Responses to broader industry challenges such as grid power availability, planning policy, reliability and move to net zero.

Statutory Framework – Scope

As per our recommendations, we think the carve-out of parts of the data centres industry as per the scope of this consultation to be unhelpful at best, and at worst, it will:

- Cause issues for the proposed registration (companies will struggle to identify if they are under scope);
- Cause issues for reporting of potential incidents;
- Risks regulatory overlap with the UK NIS Updates still in undisclosed draft; and

- Will lead to a lack of clarity over accountability in the system. This creates challenges when thinking about risk and who is accountable to these changes in the system.

Furthermore, we note that the carve-out as per the proposed scope and a focus on terminology does not address the fundamental question: Whether the services carried out in this scope are critical to national interest and whether there are risks to be addressed within the operation and management of the physical infrastructure.

Question 10: *Please share any views you may have on the definitional approach, and on the proposed indicative definitions for:*

a) data centre

We largely agree with the proposed definition of data centre, though would suggest removing the reference to the functions performed by the equipment in the data centre "providing data storage, processing and transport services" to future-proof the definition.

b) relevant data centre services

i. colocation

There are two main types of colocation:

1. Shared environments where hardware of different customers will be in the same data hall and,
2. Dedicated environments, where a single customer may lease the hall for their own purposes, but the DC operator maintains the environment as per definition of "data centre".

The definition as proposed does not clarify whether a data centre in this case would count as an "enterprise data storage" facility that is exempt or not.

ii. co-hosting

Equipment in the data centre may be placed by the provider of the data centre for their own use, but also by their customers. Where capacity on this equipment is then sold on to a third party, this is a separate service, for which the data centre is a tier 2 supplier. This type of service is typically referred to in the industry as a "cloud service", with different levels of the stack being available as entry point for purchase.

In many cases a data centre may host a range of services including co-location, bare metal hosting, private and public cloud services, which can be provided by multiple customers of the data centre, so assigning a single definition to a physical site may be difficult. It should also be noted that, a data centre provider does not usually have visibility of the kinds of services their customers provide to their consumers via the hardware that the data centre provider hosts in the data centre.

Question 11: *Please share, and explain, any views you may have on the proposed scope of third-party data centres, the operation of which are part of colocation and co-hosting services.*

As per the previous section, when it comes to equipment in the data centre, this may be placed by the provider of the data centre for their own use, but also by their customers. Where capacity on this equipment is then sold on to a third party, this is a separate service, for which the data centre is a tier 2 supplier. This type of service is typically referred to in the industry as a "cloud service provider (CSP)", with different levels of the stack being available as entry point for purchase.

In industry, data centre providers do not usually have visibility of the kinds of services that their customers provide to their customers/consumers via the hardware that is hosted in the data centre. Therefore, most colocation data centres offering this would only be able to confirm (if their sites run their own cloud service offerings), that they offer "co-hosting" as per previous definition. We note that critical users will handle their own risk mitigation strategies via suitable due diligence in procurement and via contractual methods.

Question 12: *Of the services and infrastructure that are indicated as outside the scope of the proposed framework, are there any that you feel should be included, or that you feel require a different treatment? Please explain the reasons for your answer.*

techUK notes (refer to Q4) that to drive resilience of a data centre and of a cloud services, requires different approaches and skill sets (one is largely a case of mechanical engineering, whilst the other is an IT service architecture approach), so attempting to regulate both in one approach is likely to be extremely cumbersome.

Given the industry's general aim to drive to net zero and the link between power consumption and risks around energy security, this seems to be an area missing from the considerations of the current proposals.

We would also welcome clarity on the following areas on the scope:

- For telecommunications, it appears to be a mixture of elements which are in and out of scope. For example, the consultation proposes that public electronic communications networks and services (PECN/PECS) are not in scope, but interconnection and peering is in scope. We understand this to be once again an attempt by Government to cover parts of the telecoms networks and services which may not fall in scope of the UK Telecoms Security Act, but it appears to us to only confuse matters. We note that the EU has moved PECN/PECS under EU NIS2 to ensure consistency of security rules.
- We also note the lack of clarity on whether Content Delivery Networks (CDNs) are also in scope. We note for example that CDNs are in scope of EU NIS2.
- We note that the consultation considers whether data centre owners, which could include land owners, should be within the regulatory framework, even where the data centre is operated by a third party. While it is not clear if this would simply be an obligation to appoint a regulated operator or if it would go further and require the landowner to ensure the operator meets their duties, the imposition of obligations on landowners would be a shift from the current balance of risk allocation.

Statutory Framework – Data centres and Cloud and Managed Service Providers

techUK welcomes the Government's desire to ensure that regulatory regimes are complementary rather than duplicative and have minimal overlap. The Government is right to identify the potential crossover with future updates to the NIS regulations and we agree that CSPs and MSPs should only be within scope where appropriate and within a clearly defined framework.

It is worth noting here that the public consultation on proposals to update the NIS regulations included an expansion of the current incident reporting duties beyond service continuity to include "any incident which has a significant impact on the availability, integrity, or confidentiality of network and information systems, and that could cause, or threaten to cause, substantial disruption to the service."

The need for further clarity on when such reporting duties would apply was identified in that consultation and techUK believes that DSIT should carefully consider how both sets of reporting requirements could overlap in any future framework, particularly for data centres that are leased in whole or in part by CSPs and MSPs and would remain within scope under any of the below options.

We also note the dangers of not having a clear and aligned definition of MSPs, which techUK has consistently called for both here and in the consultation on the UK NIS Updates. This is an area where industry and Government could effectively collaborate.

Furthermore, all types of regulatory reform have an impact in terms of resources. With incident reporting, an appropriate balance must be struck between the need to share information and the potential burden placed on companies dealing with an ever-growing threat landscape. It is in nobody's interest to have incident reporting requirements at a threshold where companies are submitting thousands of reports about non-critical issues. This challenge is shared by regulators who have resource challenges of their own and risk being overloaded. Effort must be focused on areas of most critical risk.

techUK believes that if the Government intends to move forward with updating the NIS regulations then CSPs and MSPs should remain outside the scope of this consultation to avoid overlapping reporting requirements and unnecessary costs for both industry and the regulator. It remains unclear how this overlap would affect CSPs and MSPs leasing space in a co-location data centre.

Statutory Framework - Mechanisms to adjust the scope

Question 16: *Please share any views you may have on the proposed power to* ***expand the scope****. We are particularly interested in information on existing or emergent forms of data storage and processing infrastructure, data centre services and connected infrastructure which may warrant future attention from the perspective of security and resilience.*

Whilst limited delegated powers are sensible to adapt to changing threats within the existing scope, changing the scope itself is far too significant a power and should be restricted to primary legislation. There should also be a statutory requirement for consultation and need to take into account innovation, economic growth and international issues.

Therefore, whilst we welcome future-proofing regulations by building in flexibility to adapt the scope, we would also caution against mixing up data centre infrastructure as a service with

definitions around the applications and services that run on the hardware hosted in data centres to avoid confusion and regulatory overlap.

Question 17: *Please share any views you may have on the proposed power* ***to exempt from scope*** *and set exemption thresholds. We would welcome any information or evidence that could be helpful for the Government to decide on any approaches to small and micro-businesses, and to small data centres, whether initially, or using the proposed power.*

If CNI or CNI style interventions are based on systemic risk due to scale and consolidation, then it is logical that smaller players would be exempt. If, however, interventions are based on criticality of service, noting the limitations that infrastructure services have in knowing the exact criticality of their customers, then it is vital that SMES are not exempt. We would welcome further clarification on the intentions and justifications of the proposed interventions on this point.

Statutory Framework - Organisations within scope

N/A.

Statutory Framework - Registration

Question 20: *Please share your views on the information that could be required at the point of registration. Do you have any recommendations for other information or data that you feel should be required?*

Registration could be beneficial, provided it is proportionate and not shared with the general public (this is a serious concern the industry has shared with the EU's Energy Efficiency Directive).

The last three points as potential information to be included at registration would bring no benefits:

- information on current customer types – Operators will apply to CNI for sites where data is hosted from customers which fall under CNI scope and have to disclose this. Therefore, this would create unnecessary duplication.
- information on risks, impacts and existing mitigations or controls – Rather we would suggest for standards to be communicated.
- information on ownership (including ultimate beneficial ownership) – We do not see benefits in volunteering such information given the existence of the Home Office FIRS scheme.

Confidentiality: Declaring customers may violate customer confidentiality, particularly demanded by critical users and any compulsion would have to be matched by a regulatory indemnity that would likely create international issues. In particular if this may be done under UK NIS Updates or through CNI registration, any information on customers should be very broad, as some operators can have hundreds of customers per individual data centre and changing every year. This could be burdensome to report on a regular basis. Furthermore, granularity of customers may be impossible to achieve, and also could prove misleading. Moreover, it is common that customer anonymity is

a contractual obligation for colocation providers. It is paramount that any regulatory powers respect client confidentiality and the primacy of freedom to contract.

We also note that there are risks of centralising security information and creating homogeneous environments.

We would also suggest limiting registration to the number of sites and geographical locations (e.g. boroughs) to help identify hot spots and those that might be impacted by a crisis / incident – otherwise it could present security posture issues.

Suggested additions

In addition to the information outlined in the consultation document, registrants could also provide information of any security and resilience testing they undertake, what scope is applied, and if this is carried out in-house or by an accredited third-party. This will support the regulator in assessing the strength of the registrant's testing regime, or whether further action is required.

Another addition which would be more beneficial than some of those included in the proposal is information about specific professional titles of employed personnel. This ensures transparency, competency, and adherence to industry standards within the organization.

Finally, registration could require details of existing standards/certifications data centres hold, which could be leveraged for compliance to the proposed framework. Of note, standard/certifications is normally publicly available information anyway.

Statutory Framework - Security and resilience measures

Question 21: *How much do you agree or disagree that the proposed mechanisms to set security and resilience measures will provide the necessary capability to address security and resilience risks, now and in the future? [scale from strongly disagree to strongly agree]*

Please explain the reasons for your answers to the previous question.

Question 22: *How much do you agree or disagree that an outcome-based approach to the baseline measures is the most effective approach? [scale from strongly disagree to strongly agree]*

Please explain the reasons for your answers to the previous question.

We note that while the consultation's narrative proposes to apply a baseline for security and resilience for data infrastructure such as data centres, this is not reflected in these questions. These are the four key components of a data centre service: Availability of power, cooling, availability of connectivity and physical security.

techUK and members broadly disagree with the proposed mechanisms as most of the topics listed (e.g. encryption, secure data, MFA, systems assessments) are more relevant to the security of data and applications, which is in the control of the application owner (mostly under cyber and GDPR), rather than the data centre provider, except where they apply to systems employed to secure and manage data centres.

In addition, there are some areas, such as third-party risk, which are not mentioned at all.

It is not clear from the list what the actual proposed measures might be in some cases, however, the list looks to be very extensive and burdensome to track if not aligned with already existing standards.

Question 23: *Please share any comments or reflections on the indicative measures, including where there may be gaps.*

We would welcome views on whether there are any areas or measures where a more prescriptive approach may be required to effectively protect or enhance security and resilience.

When it comes to cyber security, the adoption of professional titles ensures that individuals possess the expertise and competency required to effectively manage security and resilience risks within data centres. Furthermore, professional titles serve as tangible indicators of specialization and proficiency, enabling organizations to make informed decisions and allocate resources effectively to mitigate current and emerging threats. Therefore, leveraging the UKCSC professional titles as part of the proposed mechanisms will enhance the industry's ability to address security and resilience risks comprehensively.

Statutory Framework – Standards, assurance and testing

Question 25*: How much do you agree or disagree with the proposed inclusion of an earned recognition mechanism to account for existing tools used in the sector? [scale from strongly disagree to strongly agree]*

techUK broadly agrees this could beneficial and enabling providers to rely on established assurance and avoid duplication of requirements. Any mechanisms however must guard against consumers making simplistic, uninformed, or misinformed procurement decisions as a result. However, this should be based on an actual standards mechanism with proper accredited certifiers in order to be meaningful and comparable, preferably internationally recognised.

Question 26: *Please share any views on the proposed approach, and any design and implementation recommendations or suggestions you may have*

techUK and the sector welcome the focus on standards. We would recommend internationally recognized standards that are already used by the best-in-class operators. ISO (27001), and to a lesser extent national approaches like NIST make the most sense in this regard. However, we urge Government to work with industry to identify these.

The suggested framework seems to focus either on a UK approach or a greenfield approach. Anything other than the use of international standards risks fragmenting the already poor skills availability further and adds costs to UK deployment.

Therefore, techUK would welcome alignment with existing standards and accredited certifications, where the cost of implementation is reasonable for a baseline. These are both well established and recognised and alignment with standards already widely in use will reduce implementation costs, timings, as well as reduce the need for duplication. Given the international nature of several

of the data centre sector's customers, we anticipate compliance with standards to continue to be a requirement regardless of regulation.

Of note, some accreditations/certifications can have significant costs which would be prohibitively expensive for all but very large players and form a significant barrier for single-site operators. This could have unintended consequences of skewing the market and become a barrier for new entrants and innovation. We would suggest that such an "earned recognition" mechanism should be voluntary for data centre operators.

For cyber security related risks, we suggest industry-wide adoption of UKCSC professional standards.

Question 27: *Please share any views you have on this section and these topics. This may include your views on the most effective and appropriate security and resilience-related standards, certifications, assurance assessments and testing for the sector.*

Of note, EN 50600 is not a technical specification.

The adoption of UK Cyber Security Council professional standards can serve as a valuable point of reference for informing and complementing the design and implementations of proposed technical standards for data centre security. Aligning technical standards with established UKCSC professional standards will help organizations ensure workforce competence, consistency, and compatibility with recognized best practices and industry benchmarks.

Statutory Framework – Personnel

Worth noting that depending on SLAs with customers, most data centres will only allow access to personnel and staff authorised by their customers.

Statutory Framework – Incident reporting

Question 31: *Please share your views on the proposals for incident reporting to a regulator, and to other affected parties. For example, views on the proposed indicative minimum threshold and conditions.*

The proposed list of incidents is extensive and could be burdensome to report on based on some considerations.

First, the list does not appear to align with the four key elements of the data centre service as per the scope of this consultation (provision of power, network connectivity, cooling, and a secure physical environment).

Secondly, it should be noted that two key factors should be taken into consideration as making a significant difference to whether a failure of infrastructure at a data centre impacts on the availability of the services hosted on the hardware contained within the data centre:

1. How much resilience is built into the design of the physical data centre infrastructure, such as the form of battery backup and generator power to cope with a power failure.
2. How well the service has been architected for resilience e.g. by replication across several physical sites.

We strongly urge the Government to ensure that appropriate thresholds for reporting are included to limit the burden on data centre operators and the regulator alike. We suggest that only significant incidents that have an actual impact of service availability should be reportable. This would mean that certain incidents like graffiti are not reportable. We would also argue that incidents where there is no outage should not be reportable for example, a short power outage that was fully covered by back-up generators with no customer impact, should not be reportable as there would be no customer harm.

Customers: As previously mentioned, most data centre providers have visibility of incidents and/or failures that impact a data centre provider's ability to provide the physical environment for their customer's hardware. This means that while data centre providers will be able to pick by their monitoring systems attacks impacting the network connectivity to the site, they wouldn't have visibility of whether any issues actually a knock-on effect on the availability of the services provided by the costumers housed in the data centre.

Most data centre customers receive communication on incidents potentially affecting them. Furthermore, most data centre providers publish their service performance, as well as details of incidents. This is often a key commercial selling point for customers.

Data centre providers regularly conduct planned maintenance in windows of time previously communicated to customers, which allow them to take additional measures to protect the availability of their service.

Colocation customers: Colocation customers are in segregated environments, which means that any potential cyber-attack has a very limited scope to impact other users on the same site, unless the attack is directed at OT such as HVAC or security systems Given the large number of customers that colocation data providers may have (even on one site), and often this entail mandated contractual clauses, it may be unnecessarily burdensome, especially for SMEs.

Furthermore, such incident reporting may bring little value, with existing regulations and initiatives increasing the amount of information shared about key incidents. techUK has been consistent across a few consultations that thresholds for incident reporting must be set at appropriate levels which broadly meet two key tests:

1. Appropriateness. What value do these incident reports have to regulators and the wider sector they may inform? What level of risk should be reportable? The colocation provider may only understand the risk to its business, not the risk to the services provided by an impacted customer.

2. Resource Burden. Neither industry nor regulators have a dearth of staff able to easily pick up additional reporting requirements. Government needs to be able to evidence the commercial impacts that new regulations are likely to have on industry, but also on Government-funded entities which face the same resource challenges and skills shortfalls.

The largest companies in this space operate at a scale which means there is a risk they will be required to report hundreds/thousands of times on a weekly basis. This is further exacerbated by

the inclusion of reporting requirements in relation to threats and not just confirmed incidents. The complexity of these organisations needs to be more clearly taken into account. We also note that burdensome incident reporting may deter international customers from using a UK-based data centre provider where alternatives exist. The impact of any proposed regulatory changes needs to include market analysis covering what impact this might have on UK competitiveness in the sector.

Supply Chain: Most data centre providers have SLAs for their supply contracts that cover incidents and vulnerabilities notification where it is relevant to the services.

Therefore, we urge Government to consider for incident reporting whether the threshold set is relevant, and to focus on service impact of incidents which are within the control and responsibility of the data centre operator – to avoid any risk of reporting duplication. Elements on the list which might impact confidentiality and security of data is not within the responsibilities or control of the data centre operator.

Question 34: *Please share your views on public disclosure. This may include views on the process described, the parties involved, and the examples given for circumstances that could lead to a regulator considering whether the public should be informed.*

We would like further clarity on the benefit Government has identified of public disclosure of certain incidents and we would share concerns of the risks of reputational damage.

Statutory Framework – Regulatory Model and Function

Question 35: *Please share any views on the Regulatory model and function section, including the proposed supervisory and enforcement approaches.*

techUK and our members are in principle supportive of the function and principles as set out in the consultation.

However, we note that the enforcement powers seem too extensive given that users of data centres have a choice of supplier and strong commercial leavers to ensure they receive the service they require.

We also believe there to be sufficient choice in the market that any operator not meeting key requirements would have a strong commercial incentive to remedy shortcomings to prevent loss of business without regulatory enforcement.

We would also suggest that integrating professional titles into the regulatory model and function can strengthen supervisory and enforcement approaches by providing regulators with insights into the qualifications and capabilities of cyber security professionals.

Statutory Framework – Monitoring and evaluation

It is difficult to provide a useful cost estimate given the high-level nature of the proposal. We expect most operators to already have most of the required controls in place, meaning implementation costs for these may be more limited. If the reporting requirements were to be implemented as proposed, these would require additional staff and system implementation to comply.

Environmental Considerations

Question 41: *Please share your views on how to ensure unnecessary environmental harm could be mitigated where organisations are required to meet statutory requirements.*

Any policy development in regard to environmental harm reductions should be aligned with existing ESG requirements, and in alignment with the ambitious targets set by the voluntary self-regulating initiative Climate Neutral Data Centres Pact (CNDCP). The CNDCP aims to make data centres in Europe climate neutral by 2030 and includes over 100 data centre operator companies and trade associations (including techUK). The CNDCP aligns itself with the EU's European Green Deal, achieving the ambitious greenhouse gas reductions of the climate law, and leveraging technology and digitalization to achieve the goal of making Europe climate neutral by 2050.

An alternative would be to align with the EU's Energy Efficiency Directive.

If the chosen framework aligns closely with existing standards (such as ISO14001, ISO5001, SECR), the environmental impact of implementing these should be fairly low for the majority of operators. Continuity of power supply is already a key tenant of all data centre services, so it is unlikely any requirements defined under this framework would result in the increased use of fuel.

Given the strong link between power requirements and risk, it would seem amiss to not consider power usage standards as part of this framework, which could also result in environmental benefits.

General

N/A

Analysis and evidence

Question 45: *What are your views on the estimate that downtime costs the industry in the low single digit billions per year (noting that there is a wide error range around this*)?

This appears to be an overestimate and it would be helpful for DSIT to provide additional data based on a rigorous and fully disclosed methodology to justify the estimated downtime costs, as this is key to assessing the proportionality of the measures proposed in this consultation.

Data centre sites are specifically designed with increased resilience built in, so in very few cases does an outage of a particular piece of infrastructure result in the complete loss of availability of the site. In addition, any applications and services designed to best practice in resilience would utilise several different physical sites, meaning that even a compete loss of a single physical site would not impact the service availability (and data can be migrated).

In many cases, cloud-based workloads are also rapidly recoverable as cloud environments are not reliant on a single data centre site and build in resilience through redundancy and the abstraction of services from physical infrastructure. Therefore, we find the estimate in this proposal unconvincing as fails to consider the complexity of the ecosystem, from network connectivity, to different redundancy measures and levels as per SLAs, including cyber, built-in by data centres.

Question 46: *Please share your views on the drivers behind decisions to supply data centre capacity.*

Data centres tend to pick facilities around key factors such as:

1. Availability of key infrastructure such as utilities infrastructure (power, water) and at the relevant capacity;
2. Driven by customer demand;
3. Availability of land;
4. Geographical proximity to customer (ping latency) – key especially for edge.

Glossary

CSP – Cloud Service Provider

MSP – Managed Service Provider

NIS – Network Information and Security (Regulation)

CNI – Critical National Infrastructure (Designation)

CPNI – Centre for the Protection of National Infrastructure

CTP - Critical Third Party

NCSC – National Cyber Security Centre

SLA – Service Level Agreements

ICT – Information and Communication Technology

Hyperscaler – Advanced data centre facility that provides the space, power, cooling and the network infrastructure required to support the mass scale requirements of data and cloud computing.

Colo– Colocation data centre: A data centre operated by a third party with a commercial rental business model.

On-Premise – A data centre run out of an office or warehouse, usually for a single party and without the bespoke power and environmental conditions of a hyperscale or colo facility.

Contacts

Luisa Cardani
Head of Data Centres Programme, techUK
luisa.cardani@techUK.org

Lucas Banach
Programme Assistant, techUK
lucas.banach@techuk.org

About techUK

techUK is the trade association which brings together people, companies and organisations to realise the positive outcomes of what digital technology can achieve. With around 1,000 members (the majority of which are SMEs) across the UK, techUK creates a network for innovation and

collaboration across business, Government and stakeholders to provide a better future for people, society, the economy and the planet. By providing expertise and insight, we support our members, partners and stakeholders as they prepare the UK for what comes next in a constantly changing world.

techUK's award-winning Data Centres programme provides a collective voice for UK operators. We work with Government to improve the business environment for our members.

To date we've saved UK operators over £150M, alerted them to business risks, mitigated regulatory impacts and raised awareness, most recently negotiating key worker status for the sector. techUK is a signatory of the Carbon Neutral Data Centre Pact.

www.techuk.org