Microsoft's response to the Cyber Security and Resilience Bill Committee - Call for Evidence

February 2026

Microsoft welcomes the opportunity to comment on the Cyber Security and Resilience (Network and Information Systems) Bill. We strongly support the UK's efforts to modernise and strengthen its NIS Regulations framework. The Bill represents an important step toward enhancing the security and resilience of essential services and digital infrastructure across the UK. As a leading technology provider we understand the significance of risk-based, outcome-focused security practices to effectively mitigate risks and protect national interests.

Nation-states are increasingly at risk of cyberattacks due to evolving methods and diverse attackers, as highlighted in the Microsoft Digital Defence Report (MDDR). The MDDR covers a wide range of cyber threats, nation-state activities, and recommendations for improving cybersecurity defence. Nation-state actors are leveraging cybercrime to amplify their power, while financially driven cybercriminals adopt sophisticated defence evasion techniques typically seen in state operations. We continue to observe rapid changes in hybrid war tactics, election interference and a rise in ransomware and cyber-enabled financial fraud worldwide. These trends highlight the continued need to strengthen and apply effective deterrence and mitigation strategies to address these threats.

AI is transforming both the threat landscape and cybersecurity defence. We have observed threat actors using AI to enhance existing tactics, techniques and procedures of traditional cyber-attacks as opposed to creating novel threats. However, as AI systems become more capable – particularly with code-generation, autonomy and tool-call capabilities – the UK should look to draw on its talent, leadership and industry in both cyber and AI to stay ahead of these threats. AI will increasingly be an essential tool with which to counter cyber-attack, and a regulatory environment that enables the development and deployment of AI in the UK will strengthen this capability. This includes legal certainty on text and data mining for all sectors using data and innovating with AI.

As committed partners to the UK, Microsoft is dedicated to supporting efforts to combat these threats and enhance national security. We have proposed targeted refinements to the Bill to improve scoping clarity (particularly around the distinction between data centre and cloud computing services), enhance predictability and fairness in the designation of critical suppliers, and ensure that incident reporting requirements produce meaningful, actionable insights without imposing speculative or duplicative burdens.

We offer these recommendations to aid in protecting critical infrastructure and national security and maintaining a strong and resilient digital environment.

Scope and designation of critical suppliers

Microsoft broadly supports the framework for the scope and designation of critical suppliers. However, this could be improved by clarifying that data centres operating

solely as infrastructure for regulated cloud or managed services are excluded from the definition of "data centre service," avoiding duplicative oversight. We also recommend including consultation requirements, amending minimum notice periods before critical supplier designation, and strengthening rules on coordination between regulators to prevent fragmented supervision, and disproportionate administrative burdens on providers.

1. **The Bill should avoid inefficient duplication by clearly distinguishing cloud services or managed services and their supporting data centre infrastructure, on the one hand, from data centre services that are separate from cloud services or managed services, on the other. Where data centre operations constitute dedicated infrastructure for other regulated digital services, such data centre operations should not be designated for regulation separate from those other services.**

Reference: Part 2, Chapter 2, Section 15

Under the current text, it is unclear whether a cloud service's network infrastructure would be considered a "data centre service," an "enterprise" data centre operation, or simply as part of a "cloud computing service" or "managed service", particularly when a cloud service or a managed service provider uses distributed infrastructure.

The Bill defines data centre services as facilities providing IT services through physical structures housing relevant IT equipment with supporting infrastructure (Reg. 11(4)). Data centre services are defined as provided on an enterprise basis when the data centre is owned and managed by the operators exclusively for the operator's own undertaking (Reg. 11(7)) and the rated IT load of the data centre is less than 10 megawatts (Reg 11(3)).

Many cloud computing service providers, which also may offer "managed services" in conjunction with their cloud services, operate distributed data centre infrastructure solely to deliver such cloud and managed services, without providing standalone data centre services to customers (e.g., on-prem data centre solutions).

As a result, the current text runs the risk of creating duplicative, redundant, and potentially fragmented oversight, whereby cloud or managed services and their dependent infrastructure would be subject to oversight and the very same infrastructure – which exists and operates exclusively for delivery of other covered services, not data centre services to customers – would be subject to oversight as a data centre service.

The framework should instead explicitly exclude data centres operated as infrastructure for other regulated services from the definition of "data centre service," ensuring that this type of cloud infrastructure remains regulated under the cloud computing services and managed services regime rather than as a standalone data centre service. The following clarifying proviso in the definition of "data centre service," which could be added as a new Section 11(4)(c), would suffice:

> *(4) "Data centre service" means a service consisting of the provision of a physical structure (a "data centre") which—*
>
> *(a) contains an area for the housing, connection and operation of relevant IT equipment, and*

(b) provides supporting infrastructure for or in connection with the operation of relevant IT equipment.

(c) Where a provider of other services regulated under this Act operates a data centre as infrastructure for other regulated digital services, such data centre operations are excluded from the definition of data centre service.

Preserving this distinction will maintain the intended focus of the data centre service category on facilities that directly interface with end users, helping to prevent regulatory overlap and unnecessary administrative burden for cloud service providers and managed service providers operating their own infrastructure while keeping the framework coherent and proportionate.

This clarification would avoid fragmented oversight and redundant reporting obligations for managed service providers and cloud service providers operating distributed infrastructure, ensuring that the regulatory focus is on facilities directly providing services to end customers, where operational impact and continuity are most relevant and provide clarity for both operators and regulators, reducing the risk of patchwork enforcement and administrative inefficiency.

2. Critical supplier designation should be made in consultation with providers and stipulate the minimum notification period.

Reference: Part 2, Chapter 1, Section 12

The designation of a critical supplier should not be made unilaterally by the competent authority or the Information Commissioner. Meaningful consultation with the affected operator of an essential service (OES), relevant digital service provider (RDSP), or relevant managed service provider (RMSP) is essential to ensure an accurate assessment of operational dependencies.

For instance, an OES may rely on two suppliers, A and B, to maintain redundancy. In such cases, if the competent authority designates supplier A as critical without also considering supplier B it could undermine resilience planning and distort the supplier ecosystem. Where the implications of a critical-supplier designation are significant for A or B, consultation also helps maintain their ability to continue supplying the OES/RDSP/RMSP.

We therefore recommend inserting a mandatory consultation requirement with the relevant OES, RDSP, or RMSP before designating a supplier as critical under Regulation 14H.

In addition, we recommend introducing a minimum notification period under Regulation 14J(5)(a)(ii) before a designation takes effect. This would allow any allegedly critical supplier to dispute the proposed designation under Regulation 14H before it enters into force.

3. The Bill should clarify the rules governing coordination between regulators in designating critical suppliers

Reference: Part 2, Chapter 1, Section 12

Regulation 14L(1–3) rightly establishes a duty for designated competent authorities to coordinate the exercise of their functions when a person ("P") is designated under

Regulation 14H by multiple authorities, including the Information Commission. This coordination requirement is essential for ensuring consistent supervision, coherent expectations, and reduced administrative burden for regulated entities.

However, paragraph 6 of the same regulation substantially qualifies this duty by stating that the coordination obligation does not apply where compliance would impose a burden on a competent authority that is "disproportionate to the benefits of compliance." As drafted, this exemption is ambiguous and risks undermining the intended value of cross-regulator coordination—particularly for entities subject to overlapping oversight.

To prevent inconsistent interpretations of paragraph (6) and ensure coordination is not deprioritised, the following clarifications would be beneficial:

- Define who is responsible for determining when coordination would impose a disproportionate burden and set out the criteria for that assessment. A clear decision-making framework would support consistent application across authorities.
- Require the proportionality assessment to consider the wider impact on regulated entities, clarifying that the proportionality assessment must balance the administrative costs to authorities against the combined benefits of coordination—including reduced burdens on regulated entities, improved supervisory coherence, and better systemic risk management.
- Introduce a light documentation requirement when an authority relies on the exemption, ensuring transparency, accountability, and greater predictability for regulated entities.

These clarifications would help preserve effective cross-authority coordination while ensuring the exemption is applied in a balanced and consistent manner.

Incident Reporting Obligations

Microsoft supports mandatory incident reporting obligations that increase transparency and help to improve response across organisations impacted by an incident. We recommend that the Bill sets clearer criteria for what constitutes a significant incident, excludes reporting of 'potential misses', adjusts reporting timelines, and clarifies reporting obligations between service providers and customers. We also recommend aligning reporting requirements with international standards and establishing reporting reciprocity across jurisdictions to prevent duplication for UK businesses, foster international cooperation, and optimise resource allocation.

4. The Bill should retain the original definition of "incident" under the NIS Regulations, which limits "incident" to events that actually occur and have an adverse effect.

Reference: Part 2, Chapter 2, Section 15

We recommend retaining the original NIS definition, which limits "incident" to events that actually occur and have an adverse effect.

Regulation 15(2) expands the definition of an "incident" to include any event capable of having an adverse effect on the operation or security of network and information systems.

This proposed definition is broad and speculative. Once potential events fall within scope, operators must assess countless routine defensive actions under a subjective "capable of having an adverse effect" test, creating high volumes of low-value reports that obscure genuinely significant incidents and weaken, rather than improve, oversight. Moreover, relying on future secondary legislation to filter these reports is insufficient, as the reporting burden begins with the definition itself, not the significance criteria.

For example, a cloud provider that blocks millions of credential-stuffing attempts daily could be required to report each automated block as a "potential miss," generating thousands of non-actionable notifications. Similarly, a managed service provider that blocks large phishing campaigns could face an obligation to report every attempted campaign – even when fully mitigated – flooding authorities with noise that displaces meaningful signal.

Assessing whether an event was merely "capable" of causing harm will lead to inconsistent interpretations across sectors, while diverting resources away from real incident response toward compliance-driven speculation.

5. **The Bill should clarify that an entity has the right to promptly conduct a reasonable investigation of incidents and determine and assess elemental facts before it becomes "aware" of a significant incident and incurs a duty to report.**

Reference: Part 2, Chapter 2, Section 15

Under proposed Regulation 11(2), 11A(2), 12A(1), and 14E(1) the relevant entities are required to report an incident when they become "aware" that the incident has occurred or is occurring. But the law does not explain what constitutes awareness triggering a reporting obligation. Clarification of this pivotal element is critical for establishing a clear, consistent obligation and for operationalising incident response and reporting procedures and, ultimately, timely situational awareness among regulators.

The Bill should clarify that awareness of a reportable incident presupposes that an entity has collected and assessed relevant information against the criteria set out in the Bill and has determined that the applicable triggering thresholds have been met. This investigative process, including the time to assess information, will vary depending on the circumstances of an incident.

6. **The Bill should amend the 'data centre incident' definition to ensure it captures actual service or system failures, not near misses, and remove obligations that require operators to assess UK-wide impacts beyond their visibility.**

Reference: Part 2, Chapter 2, Section 15

The proposed definition of a "data centre incident" in Regulation 11(A)(3) includes incidents that *"could have had"* or *"are likely to have"* significant impacts. This formulation risks capturing near misses and routine continuity events that are fully mitigated by redundancy. Modern data centres are engineered to absorb disruptions by design; reporting such events would produce high volumes of low-value notifications and divert attention from genuinely critical incidents.

Moreover, modern data centres are designed with redundancy and failover mechanisms to absorb disruptions. Incidents fully mitigated by these systems demonstrate resilience,

not failure. Treating such events as reportable may mischaracterise normal operations and ultimately weaken overall system reliability.

The current wording, which encompasses incidents that "*could have had or are likely to have"* significant impacts, will likely result in a flood of near-miss reports. This could overwhelm competent authorities and CSIRTs, producing little actionable intelligence, while imposing administrative burdens that distract operators from effective incident response, potentially undermining security.

To ensure proportionate and actionable reporting, data centre operators should be required to report only actual incidents affecting the operation, security, or continuity of the data centre services they provide - not hypothetical, speculative, or fully mitigated events. The obligation should also be limited to impacts on the operator's own systems and services, as data centre providers typically do not have visibility into customers' architectures, redundancies, or the broader implications of customer-side failures. They should therefore not be required to assess "any other significant impact on the UK," as currently set out in point Regulation 11(A)(3)(c).

OES providing data centre services should not be required to assess the impact to the UK beyond the services they provide directly to their customers. They may not have accurate insights into what services or redundancies their customers have.

We recommend amending the data centre incident definition in 11A(3) as follows:

> *11A (3) In this regulation, "data centre incident" means an incident which ~~could have had,~~ has had* ***or*** *is having ~~or is likely to have—~~*
>
> *(a) a significant impact on the operation or security of the network and information systems relied on to provide the data centre service provided by the OES in the United Kingdom*
>
> *(b) a significant impact on the continuity of the data centre service provided by the OES in the United Kingdom* ***outside of anticipated operating conditions and planned maintenance activities****.*
>
> *~~(c) any other impact, in the United Kingdom or any part of it, which is significant.~~ "*.

7. The Bill should introduce clear availability metrics based on performance level, not broad concepts of "disruption" or 'duration of the incident'.

Reference: Part 2, Chapter 2, Section 15

To ensure that the "extent of disruption" in *Regulation 11(4)(a), 12A(3)(a)* and *14E(3)(a)* has operational meaning and prevents over-reporting of immaterial service reductions, the Bill should adopt performance-level degradation as the metric for availability, similar to industry-standard SLAs.

For OES, RDSPs, and RMSPs, "extent of any disruption" and "duration of the incident" are listed as significant factors *(Regulation 11(4)(a)–(c), 12A(3)(a)–(c), and 14E(3)(a)–(c))*. As drafted, any actual and likely decline in performance could be interpreted as "disruption," even when the degradation is minor, brief, or has no material impact on users. We recommend using service-level reduction data and percentage of customers impacted as alternative criteria to the user-hour metric.

8. The Bill should clarify that providers may rely on enterprise customer data when individual user numbers are not known.

Reference: Part 2, Chapter 2, Section 15

Significance factors for *OES (Regulation 11(4)(b)),* RDSPs *(Regulation 12A(3)(b))*, and RMSPs *(Regulation 14E(3)(b))* require assessing "number of users [...] affected." However, for many cloud and managed services, providers cannot know the number of natural-person users within an enterprise tenancy; only the customer has that information.

We recommend amending the significance factors to clarify that when regulated entities lack reliable data on natural-person users, they may assess impact based solely on the number of enterprise customers, tenants, or contracted accounts. "Users" should be explicitly understood to include enterprise accounts, not only individual natural persons. This ensures entities are evaluated on information actually available to them, aligning with operational realities.

9. The Bill should refine the data-compromise criterion to avoid overbroad reporting obligations

Reference: Part 2, Chapter 2, Section 15

For OES *(Regulation 11(4)(e)),* RDSPs *(Regulation 12A(3)(e)),* and RMSPs *(Regulation 14E(3)(e))*, any actual or likely compromise of "confidentiality, authenticity, integrity, or availability of data relating to users" may contribute to significance. As written, this could capture compromise of internal, non-sensitive operational data, require reporting of incidents affecting one user with no broader societal or systemic impact, and trigger reports even where the data's connection to the service is minimal ("data relating to users").

The Bill should refine the factor so that reportability hinges on materiality of the compromised data (e.g., sensitive, regulated, or impactful data), impact on actual service delivery or user security, scope and potential harm beyond a single user. Moreover, exclude cases where user data 'is likely to be compromised'.

Suggested amendments to Regulation 11(4)(e), 12A(3)(e)), and 14E(3)(e):

> ***"****(e) whether the confidentiality, authenticity, integrity or availability of data relating to users of the relevant digital service has been~~,~~* ***or*** *is being ~~or is likely to be~~ compromised;* **to the extent that such information is *reasonably available to the entity based on the data it possesses* regarding its customers. Where entities do not possess information relating to individual end users, they may rely exclusively on information concerning customers with whom they have a direct contractual relationship.***"***

10. The Bill should remove the criterion of "impact on the economy or society" for RDSPs and RMSPs.

Reference: Part 2, Chapter 2, Section 15

For RDSPs and RMSPs, the UK Bill introduces a significance factor requiring assessment of: "any impact that the incident has had, is having or is likely to have on the economy or the day-to-day functioning of society." (Regulation 12A(3)(g) and 14E(3)(g)). This factor is not included for other OES. Its inclusion for RDSPs/RMSPs creates several issues:

- **Disproportionate and inconsistent obligations**: RDSPs and RMSPs would face a broader and more speculative set of reporting triggers than any OES category, despite being subject to the same overarching NIS framework. This expands reporting beyond service-related impact into macro-level socio-economic consequences - a level of assessment not required of energy, transport, health, data centre operations, or other OES sectors.
- **Speculative and unworkable assessments:** Providers generally cannot accurately determine economy-wide or society-wide consequences of a technical incident. This risks over-reporting, as cautious providers may submit notifications in the absence of any reliable method to assess national-level downstream effects.
- **Divergence from the Bill's core structure:** All other significance factors focus on direct, measurable impacts: disruption, users affected, duration, and data compromise. The economy/society criterion is the only one requiring hard to inference about and hard to quantify downstream societal effects, with no defined threshold.

11. The Bill should remove the criterion of "the geographical area which has been affected, is being affected or is likely to be affected by the incident;" for RDSPs and RMSPs.

Reference: Part 2, Chapter 2, Section 15

For RDSPs and RMSPs, the UK Bill introduces a significance factor requiring assessment of:

> *the geographical area which has been affected, is being affected or is likely to be affected by the incident; (Regulation 12A(3)(d) and 14E(3)(d))*

Providers generally may not be able to accurately determine the geographical impact of an incident.

12. The Bill should clarify the reporting responsibilities between service providers and their customers, in particular in the context of cloud computing services and data centre services provisions

Reference: Part 2, Chapter 2, Section 15

We recommend that reporting responsibilities among providers and their customers are clarified, including in the context of cloud services.

The use of cloud services is governed by what is referred to as a "shared responsibility matrix". Depending on the nature of the service, the cloud service provider is responsible for certain elements, such as the operation and security of the underlying cloud infrastructure, while the customer is responsible for configuring the service, managing its data and the interoperation of the cloud service with other IT services (either additional cloud services or on-premises technology). In the case of detection of an incident that is targeting an essential service provider who is the customer of a cloud service provider, it is typically only the customer, and not the cloud service provider, that is able to determine what information is the target of such a threat or the criticality of the targeted systems to the operation of that essential service provider. This is why we recommend creating policies and protocols that reflect the inherent lack of cloud provider visibility into the

significance of incidents impacting cloud customers (as well as lack of cloud provider control over the behaviour of cloud customers, which retain an important role in security and resiliency responsibilities, either separate from or in coordination with their cloud service providers).

We also recommend clarifying in the text of the proposal that, in case of incidents affecting entities using cloud services, the reporting obligation lies on the entity with visibility into the incident's significance unless the incident is the result of an actual vulnerability within the underlying cloud infrastructure controlled solely by the cloud service provider.

Based on the potential for confusion, the Bill needs to set forth clear criteria for determining when a cloud service provider must report an incident, as compared to when an incident must be reported by an entity using cloud services. This clarity is critical not only for cloud providers but also for cloud customers with uncertainty about what is being shared about them and with a responsibility to report incidents impacting their operations and areas of risk management ownership.

Functions of competent authorities and CSIRT in relation to notified incidents

Microsoft supports the Bill's objectives on incident reporting, information sharing, and improving collective cyber resilience, particularly requirements that enable authorities and CSIRT to share incident information to prevent wider harm and support coordinated response across the sector. However, the Bill could be improved by extending consultation requirements to disclosures made to other regulated persons, ensuring providers are not identified without consent.

We also recommend introducing a "report once" mechanism to eliminate duplicate incident submissions and enabling reporting reciprocity with international regimes such as the EU's NIS2, reducing the administrative burden while supporting timely, effective incident response.

13. The Bill should mandate consultation with providers providing incident notification before disclosing incident notifications information to other regulated persons.

Reference: Part 2, Chapter 2, Section 15

We recommend that the principle of consultation with the provider before sharing information, which already applies in the context of public disclosure under regulations 11B(7)(b), 12B(5)(b), and 14F(5)(b), be extended to disclosures to any regulated person under regulations 11B(9), 12B(7), and 14F(7).

Specifically, before a designated competent authority, the Information Commission, or the CSIRT shares information from a notification to prevent other similar incidents, the relevant OES, RDSP, or RMSP should be consulted to confirm that the information to be shared does not identify them without their consent. This extension would align the practice of sharing information for incident prevention with existing protections for public disclosure, ensuring that providers' identities are safeguarded while allowing authorities and CSIRT to share relevant information to help prevent similar incidents across the sector.

14. Establish a "report once" mechanism and remove duplicate-submission requirements.

Reference: Part 2, Chapter 2, Section 15

The Bill currently requires entities to submit incident reports to multiple authorities. For example, RDSPs must notify the competent authority and also send *"a copy of the notification"* to the CSIRT (*Regulation 12A(7*)). RMSPs face the same obligation (Regulation 14E(7)). Equivalent duplication appears in the OES and OES–data centre provisions (*Regulation 11(8)* and *11A(7)).*

This approach imposes unnecessary burden during incidents and fragments the government's situational awareness, as different authorities may receive information at different times or in different forms. It is also misaligned with emerging best practice across jurisdictions, which increasingly favour single-entry reporting with centralised dissemination.

We recommend amending regulation *11(8), 11A(7), 12A(7),* and *14E(7)* to replace the requirement for entities to send "a copy" of the incident notification to another authority with a unified *report once* mechanism. Entities should submit a single notification to the UK CSIRT, which would then be responsible for transmitting it to the relevant competent authority or authorities. The legislation should confirm that submission to the CSIRT fully satisfies the reporting obligation under each regulation. A single-entry model would reduce administrative pressure on regulated entities during critical response moments, ensures consistent and synchronised information across government bodies.

15. Promote incident reporting reciprocity.

Reference: Part 2, Chapter 2 (general)

While Microsoft supports incident reporting requirements, overlapping reporting requirements across jurisdictions can complicate compliance and divert resources, potentially hindering effective incident response. The Bill offers an opportunity to combat inefficiencies by aligning reporting requirements with international standards and allowing reporting reciprocity between jurisdictions.

The European Union's update to *The Network and Information Security (NIS2) Directive* establishes mandatory reporting requirements for significant cybersecurity incidents impacting essential and important entities within the EU.

The Bill should permit reports prepared for NIS2 compliance to be accepted for the UK's reporting requirements. This reciprocity would prevent duplication of efforts and foster better international cooperation and resource allocation.

The Bill's reporting timelines should either mirror or provide greater time than those set by the NIS2 Directive, to ensure sufficient time to gather information. Allowing reports prepared for NIS2 to be accepted for the UK's reporting requirements will prevent duplication of efforts for UK businesses, foster better international cooperation, and optimise resource allocation.