# National Grid

## Cyber Security and Resilience Bill
## Written Evidence

**February 2026**


### Summary

National Grid sits at the heart of Britain's energy system, connecting millions of people and businesses to the energy they use every day. Our approach to cyber resilience is proactive and risk-based, blending robust engineering standards with modern cyber-security practices to protect our operational systems and data against evolving threats. We work closely with Government, regulators, industry and our supply chains to ensure that threats are identified early, managed consistently and mitigated effectively.


The Cyber Security and Resilience Bill ('the Bill') is a crucial piece of legislation that will help modernise cyber regulation in the UK and boost the resilience of services and infrastructure critical to the country's economic and physical security. We support the overarching aims of the Bill, particularly the extension of regulation to manufacturers and critical suppliers, however measures must be implemented in a coordinated way, with clear definitions and unambiguous guidance for industry. To be effective, the Bill will need to achieve the following objectives:

1) Deliver targeted and effective regulation of supply chains and manufacturers
2) Clarify new definitions for incident reporting, ensuring they are consistent and proportionate
3) Define delivery responsibilities and ensure regulators have the resource to effectively enforce regulations
4) Establish an enduring and agile Cyber Security and Resilience framework

### Deliver targeted and effective regulation of supply chains and manufacturers *(Clauses 12-14)*

- While there is no direct change for energy networks, which are currently regulated under the existing Network and Information System (NIS) regulations, the expansion of the framework to bring manufacturers, supply chains, and data service providers into scope is a welcome one.
- Bringing supply chains into scope of the existing NIS framework will reduce the inherent knock-on risk on Operators of Essential Services (OES) such as energy networks, while also serving to boost the baseline cyber resilience of regulated companies.
- Under current regulations, there is no legal obligation on manufacturers to follow the same cyber-resilience standards as OES, which can cause an imbalance where regulated organisations are held to stringent NIS-aligned security obligations, yet components they rely on are produced by suppliers outside of regulatory frameworks. This is particularly exacerbated within the energy sector, where companies are restricted to a small supply chain due to high competition for raw materials.
- Proposals set out in the Bill to bring supply chains and manufacturers designated as "critical suppliers" into scope of regulations rectify this imbalance and we welcome these reforms. However, moving forward we must be cognisant of how "critical suppliers" are designated, as any misclassification could expose OES to avoidable supply-chain cyber risk.
- OESs will need to continue to rigorously map and manage supply chain risk, particularly providing sufficient visibility of critical dependencies in order to support regulatory engagement in the designation of "critical suppliers," even though the primary compliance burden will now sit with "critical suppliers" themselves.
- Given that "critical suppliers" will be designated based on the potential impact of their disruption on OES, rather than the scale of their operations, the Bill should consider how targeted support for Small and Medium Enterprises (SMEs) could help them meet new cyber security requirements, should they be designated as "critical suppliers."
- While there will be a new cost of compliance for all designated "critical suppliers," this could disproportionately impact SMEs with limited cyber maturity, making targeted support for these firms a key enabler of effective compliance.

### Clarify new definitions for incident reporting, ensuring they are consistent and proportionate *(Clauses 13-16)*

- The Bill will expand current reporting requirements, instituting a new two-stage reporting structure that will require regulated entities to notify their regulator of a significant incident no later than 24 hours after becoming aware of that incident, followed by a full report within 72 hours.
- The Bill also broadens the definition of a reportable incident, setting out a deliberate aim to capture more incidents which may have compromised the integrity or security of a system in a way which could have future impacts. This is a significant shift from current regulations, where reporting decisions are dictated by tangible impact on current systems.
- The Bill must clearly define what constitutes a reportable incident. This definition should remove any ambiguity from the reporting framework, while ensuring that reporting is applied consistently and proportionately and focussed only on the incidents that pose a genuine risk to the resilience of the regulated system.
- Moving from an outcome-based system of reporting to a more speculative one could result in cyber security functions reporting minor security events not initially envisaged by the Bill, with capacity being stretched thin on minor incidents and a dilution of focus on legitimately critical incidents.
- At the current level of detail set out in the Bill, the reporting measures lack clear boundaries or criteria setting out exactly what level of incident will need to be reported, and when considered in tandem with the shortening of timescales for reporting, could lead to significant stresses on regulated organisations' cyber security functions.
- Expanding the definition of reportable incidents would impact all cyber security functions, with Government and regulators likely forced to consider a volume of incidents beyond which their staff can reasonably process, similarly risking that insufficient attention is given to genuinely critical incidents.

### Define delivery responsibilities and ensure regulators have the resource to effectively enforce regulations *(Clauses 29-35)*

- The Bill will fundamentally change the landscape of national cyber security regulation, and the new regime will require a clear delineation of duties between the Department of Science Information and Technology (DSIT), Department for Energy Security and Net Zero (DESNZ), the National Cyber Security Centre (NCSC), and regulators.
- Most prominently, the Bill significantly boosts the role of regulators, expanding powers to proactively gather information, and punitive abilities to enforce penalties. We welcome this expanded role for regulators and believe it can strengthen the overall effectiveness of the regime. However, in order to fully realise this role, regulators must hold the necessary expertise and capacity so that enforcement actions, including financial penalties, can be applied effectively and consistently.
- There is potential for an increase in duties to place significant pressure on regulators with varying levels of cyber expertise, which could lead to a heightened risk of enforcement actions, particularly financial penalties, being applied inadvertently or disproportionately.
- It is therefore vital that regulators be appropriately staffed with suitably qualified and experienced personnel or there is a risk that new powers are utilised incorrectly or not utilised at all. Given the NCSC will retain its position as the primary technical authority, close collaboration between the NCSC and regulators will be required to ensure that this technical expertise is reflected in the day-to-day operations of regulators.
- Support will also be required to ensure consistent interpretation between government departments and regulators, including standardised policy, guidelines and templates, and consideration should be given as to whether this function could be delivered centrally. Early-stage engagement with industry will be key to avoid misalignment or disproportionate enforcement, while regulated organisations will require clarity to embed the new processes required to meet heightened requirements.

### Establish an enduring and agile Cyber Security and Resilience framework in partnership with industry *(Clauses 36-42)*

- We welcome provisions within the Bill to grant the Secretary of State new powers to update cyber security regulations through secondary legislation as opposed to new primary legislation.
- Cyber security is a fast-evolving landscape, and a more agile national framework will ensure that the UK is able to better react to emerging threats at pace.
- However, legislation must strike a balance between remaining agile, and the need for appropriate consultation on new or enhanced duties for regulated organisations.
- We would particularly value the opportunity to engage on any future changes to reporting thresholds or definitions which could impose significant new duties for cyber security functions on short notice. Implementing these

changes unilaterally without industry having forward visibility would risk stretching cyber security capacity, potentially diverting attention from potentially system-critical incidents.