ofgem
Making a positive difference for energy consumers

UK Government

Reshaping Cyber Regulation in Downstream Gas and Electricity

Consultation

Closing date: 22 May 2026

Department for Energy Security and Net Zero (2026)

Contents

Foreword

Cyber security is of utmost and growing importance to today's Government. The National Cyber Security Centre (NCSC) now warn that we face four nationally significant cyber-attacks every week. Last year, NCSC handled the highest number ever of nationally significant cyber incidents (204 compared to 89 the year before). Nearly half of incidents requiring NCSC support were related to national infrastructure[1]. Alongside this, Great Britain (GB) is racing towards net zero, resulting in the rapid transformation of our energy sector. New technologies are emerging, assets are being decentralised, and energy sources are becoming more distributed. With every aspect of our society relying on a strong and reliable energy system, our Downstream Gas and Electricity (DGE) operators must be resilient to evolving cyber threats.

In 2018, when the Network and Information Systems (NIS) Regulations were brought in, our strategic approach to energy resilience was focused on the largest operators who provided the majority of gas and electricity services to GB[2]. The composition of the system is changing now, so that a broader range of organisations play an increasingly important role in delivering energy services and system balancing. Therefore, it is time for us to reconsider our approach to cyber resilience.

To protect consumers, reach our net zero goals and maintain a strong, resilient energy network, cyber security is essential. System-wide cyber resilience is increasingly important, particularly at this time of heightened geopolitical uncertainty, as the threats that we face are evolving. The protection of, not only our essential services[3], but also our businesses, is key. As demonstrated by the recent cyber-security attack on Polish energy infrastructure, the entire energy system is an attractive target for adversaries, and all sizes of organisation should have protective measures in place. Our cyber security approach needs to keep pace to reflect these evolving risks, and there is a clear need for the Government and the regulator to support the energy sector in doing so.

Our proposals in this consultation are aimed at increasing the resilience of energy businesses against cyber adversaries and protecting the British energy system. We propose to do this by ensuring that all Ofgem licensees have baseline cyber resilience in place, while reviewing the cyber regulatory framework to ensure it still captures to the most critical DGE operators for the transforming energy system. Through this approach, no Ofgem licensee will be unprotected, and the most critical operators will be subject to the highest resilience requirements, as is appropriate. Ultimately, we want to protect the country's security of supply to ensure consumers' lights stay on and homes stay warm, and safeguard against the mounting economic impacts of cyber-attacks.

[1] UK experiencing four 'nationally significant' cyber... - NCSC.GOV.UK
[2] Whilst the Network and Information Systems Regulations 2018 apply UK wide, Ofgem and DESNZ regulate energy in Great Britain. The Department of Finance for Northern Ireland regulates in Northern Ireland.
[3] essential service means a service which is essential for the maintenance of critical societal or economic activities

Through this public consultation, you can contribute your views to help us shape future policy and tackle the cyber security challenges facing the energy sector so that together we can maintain a secure and resilient energy system.

Minister Shanks
Minister of State for Energy

Mark McAllister
Chair of Ofgem

General information

Why we are consulting

This consultation has the following objectives:

- Seek views on whether stakeholders agree there is a need to change how cyber resilience requirements apply across DGE.
- Invite feedback and evidence on two proposals for change:
    - The introduction of baseline cyber resilience requirements for all Ofgem licensees and
    - The expansion of the scope of the NIS Regulations for DGE, by amending the NIS criteria for designation.

We welcome feedback and evidence from a range of stakeholders; including from licensees, developers and industry bodies to think tanks and academia, to inform the development of our proposals. Your input will be vital in shaping requirements that are appropriate, future-proof, protect businesses, and are effective in defending against an evolving and complex, threat landscape.

The proposals and questions in this consultation relate to operators and organisations delivering services in the DGE sector in Great Britain.

Consultation details

Issued: 27 March 2026

Respond by: 22 May 2026

Enquiries to:

Cyber Policy Team
Department for Energy Security and Net Zero
Old Admiralty Building
London
SW1A 2EG

Email: cyber.policy@energysecurity.gov.uk

Cyber Strategy Team
Ofgem
10 South Colonnade
Canary Wharf
London

E14 4PU
Email: CyberStrategy@ofgem.gov.uk

Consultation reference: Reshaping Cyber Regulation in Downstream Gas and Electricity

Audiences:

This consultation will be of interest to companies and trade associations in the DGE subsector, and those working with Ofgem licensees.

Territorial extent:

Great Britain

How to respond

Respond online at: https://energygovuk.citizenspace.com/energy-security/whole-energy-cyber-resilience-requirements

When responding, please state whether you are responding as an individual or representing the views of an organisation.

Your response will be most useful if it is framed in direct response to the questions posed, though further comments and evidence are also welcome.

DESNZ and Ofgem will share all responses received with each other.

Confidentiality and data protection

Information you provide in response to this consultation, including personal information, will be available to both DESNZ and Ofgem and may be disclosed in accordance with UK legislation (the Freedom of Information Act 2000, the Data Protection Act 2018 and the Environmental Information Regulations 2004).

If you want the information that you provide to be treated as confidential please tell us, but be aware that we cannot guarantee confidentiality in all circumstances. An automatic confidentiality disclaimer generated by your IT system will not be regarded by us as a confidentiality request.

We will process your personal data in accordance with all applicable data protection laws. See our privacy policies: DESNZ privacy policy, Ofgem privacy policy. Unless otherwise stated against specific questions, we will summarise all responses and publish this summary on GOV.UK. The summary will include a list of names or organisations that responded, but not people's personal names, addresses or other contact details.

Quality assurance

This consultation has been carried out in accordance with the government's consultation principles.

If you have any complaints about the way this consultation has been conducted, please email: bru@energysecurity.gov.uk.

The proposals

Background

Threat landscape and the composition of the sector

The Government's Clean Power 2030 ambitions are projected to significantly change the energy technology landscape. This expansion in energy infrastructure and connectivity changes the risks across the system. Battery storage capacity is projected to see a six-fold increase, while the UK's wind and solar capacities are expected to almost triple, by 2030[4]. These projections are actively driving a surge in planning applications for new developments in these sectors[5]. It is important that new operators ensure their infrastructure is secure by design when scaling up their operations. Embedding security and resilience consistently into energy sector operations now, will prevent a retrospective and costly security debt later.

The cyber threat landscape is also changing. The UK Government's most recent Cyber Security Breaches Survey (2025) shows attacks are occurring regardless of organisation size, as adversaries often act opportunistically and target the weakest link. It found that 41% of micro, 50% of small, 67% of medium-sized and 74% of large businesses reported experiencing any kind of cyber security breach or attack in the last year[6]. A separate report commissioned by the Department for Science Innovation and Technology (DSIT) conducted by KPMG on 'Economic modelling of sector-specific costings of cyber attacks' (2025), estimated that the average cost of a significant cyber-attack in the utilities sector exceeds £210,000[7]. We recognise that these figures are based on US data and are not sector specific, as they combine both the water and energy sector for utilities. However, we consider them to be adequate to indicate a need for change[8]. We will use this consultation as means for gathering UK sector specific information for energy. There are also more organisations participating in the energy ecosystem than ever before, and in different ways, to help manage a much more complex landscape as we integrate renewables and build energy independence. This means what we view as critical has changed, as the system becomes less concentrated. Ofgem and DESNZ therefore consider it no longer sufficient to focus cyber resilience requirements solely on a subset of large operators.

[4] NESO advice on achieving clean power for Great Britain by 2030
[5] Renewable Energy Planning Database: quarterly extract - GOV.UK
[6] Cyber security breaches survey 2025 - GOV.UK (figure 4.1). The prevalence of cyber security breaches or attacks amongst businesses has seen a decline from 2024, down from 50% in 2024 to 43%.
[7] Economic Modelling of sector specific costings of cyber 2025 (table 1.1). Average costs across all firms in the utilities sector including electric power generation, transmission and distribution, natural gas distribution and water, sewage and other systems. Average costs range from £93,665 for a micro organisation to £436,443 for a large organisation. Figures are in 2024 prices.
[8] The KPMG Report on 'Economic Modelling of sector specific costings of cyber 2025', uses the NAICS utilities definition that includes energy, water and sewage services. We consider these to be directly comparable to DGE considering their nature and technology in use. North American Industry Classification System (NAICS) U.S. Census Bureau

The cyber threat to the UK's CNI has continued to increase and the NCSC has been emphasising the need to close the widening gap between the escalated cyber threats to critical services, and our collective ability to defend against them[9]. As a key part of the CNI sector, the DGE system could be a high-value target for cyber adversaries.

Energy underpins our way of life and is vital to all other critical national infrastructure sectors. Disruption in the energy system can quickly lead to cascading impacts and significant disruption to businesses and households. The fire at North Hyde Electricity Substation in 2025[10], whilst not a malicious attack, is a clear example of how this can play out in practice. Though power was restored within hours, secondary impacts to the aviation sector due to the associated closure of Heathrow Airport continued to be felt for days. Energy companies and their supply chains are therefore an attractive target for maximising disruption, and increasing digitalisation and interconnectivity across the energy system increases the exposure to attack.

Recent cyber-incidents affecting the energy renewables sector, as well as the widespread occurrence of high-profile ransomware incidents, reinforce the urgency for improved system-wide cyber defences. The recent attack on the Polish energy system is clear evidence of adversaries' shifting focus. In December 2025 a threat actor targeted around 30 distributed renewables assets, including wind and solar farms, a combined heat and power plant, and a company in the manufacturing sector[11]. Whilst it was ultimately unsuccessful in disrupting energy supplies, it could have impacted over 500,000 customers. The attack demonstrates a clear move towards coordinated disruption to the energy sector through distributed renewable assets and both IT and OT[12] environments. This was not deemed to be a sophisticated attack; the actor was able to use a variety of vulnerabilities and circumnavigate weak defences to infiltrate systems, most of which could have been prevented by cyber hygiene.

Regulatory environment

The NIS Regulations establish a framework to boost the cyber resilience of operators of essential services, the thresholds for which were set in the NIS Regulations[13]. For DGE, Ofgem and DESNZ are a joint Competent Authority under NIS and have issued guidance to the sector on NIS implementation[14,15].

On 12 November 2025, the Government introduced to Parliament the Cyber Security and Resilience (Network and Information Systems) Bill (CSRB)[16], to address specific cyber security challenges faced by the UK. This includes a number of specific changes to the existing NIS regulatory framework. The CSRB seeks to give the Government greater flexibility to regulate network and information systems and better equip regulators with additional tools to strengthen the resilience of essential services. The Bill introduces essential powers that strengthen the

[9] CAF v4.0 released in response to growing threat | - NCSC.GOV.UK
[10] North Hyde Substation Incident - 20th March 2025 | National Grid
[11] Energy Sector Incident Report - 29 December 2025 | CERT Polska
[12] Operational Technology, meaning technology that manages physical processes, machinery and industrial equipment.
[13] NIS Schedule 2 - Essential Services & Thresholds
[14] NIS Directive and NIS Regulations 2018: Ofgem guidance for Operators of Essential Services | Ofgem
[15] DESNZ Policy Guidance for the Implementation of the Network and Information Systems Regulations
[16] Cyber Security and Resilience Bill

overarching framework and lay the groundwork for further reform, including powers to amend the NIS framework. These powers unlock the proposals set out in this consultation by providing the regulatory levers required to review NIS applicability. This will in turn drive further improvements in the resilience and security of DGE.

Section 1: Proposed Approach

We have identified two risks with the existing cyber regulation and oversight approach in DGE.

- The coverage of the NIS Regulations. There is a risk that the essential services in scope and associated thresholds, have not kept pace with the changing threat and energy landscape.
- The lack of cyber requirements for organisations outside of the scope of the NIS Regulations, despite their increasing importance for the energy system.

Therefore, to address these issues, we are proposing two approaches:

- **Reviewing NIS applicability**: Revise scope of the current regulatory framework (the NIS Regulations) to ensure DGE operators that can materially impact energy system stability fall within the regulatory scope. This would be subject to CSRB enactment.
- **Baseline requirements**: Ensure all Ofgem licensees have a baseline level of cyber resilience in place, using requirements that are not burdensome to implement but provide resilience against the most common cyber-attacks.

This should reflect the evolving cyber threat landscape and the shift from a traditional reliance on major players, to a system that depends on more diverse and distributed operators. By ensuring every licensed organisation establishes and maintains a baseline level of cyber security, we reduce the likelihood of opportunistic attacks from threat actors, strengthening the protection of businesses and services delivered in the sector. This benefits both individual companies, and the security and resilience of the services that are essential to the UK economy and society.

We recognise the significant gap between NIS requirements (high-impact operators captured under the NIS Regulations) and baseline requirements for all Ofgem licensees. Our proposal is to implement and assess this model before considering whether any further proportionate requirements should be implemented in between baseline and NIS requirements. Through this consultation, alongside seeking feedback on our two proposals for change, we wish to gauge appetite as to whether in the future we should consider further targeted policy work, and any future intermediate requirements. While we do not propose to consider intermediate requirements until after the baseline requirements have been implemented and the NIS applicability has been reviewed, this consultation will help us understand early stakeholder feedback on their merits.

Proposed Approach Questions

With the proposal in mind, we welcome your feedback through the following questions:

1. **Is there a need to expand the scope of our cyber oversight and assurance to cover more DGE operators? Please provide further detail on why.**

2. **If you answered yes to question 1, what are your views on our proposal to expand the scope of our cyber oversight and assurance to cover more DGE operators by: (a) reviewing who NIS applies to and ensuring the most critical DGE operators for the increasingly distributed and digitalised energy system fall within its scope and (b) introducing baseline cyber resilience requirements for all Ofgem licensees?**

3. **Are there any alternative approaches we should consider on how to expand the scope of our cyber oversight and assurance and build resilience across the sector, whilst maintaining strong cyber security measures for critical operators? Please explain your reasoning.**

4. **Do you think there is a need for intermediate cyber requirements (above baseline but below NIS) in DGE? If so, do you think these should be considered in a staged approach (implementing baseline requirements for all Ofgem licensees and reviewing NIS applicability first before proceeding to scoping intermediate requirements)? Please explain your reasoning.**

5. **If you think there is a need for intermediate requirements, what risks should they look to address and who should they target?**

Section 2: Reviewing NIS Applicability

Revise the NIS Regulations thresholds and essential services for DGE

Currently, organisations are brought in scope of the NIS Regulations by either meeting a relevant threshold for the service they provide[17], or being designated by regulators due to their significance, even if they do not meet defined thresholds[18]. Existing regulatory coverage may not accurately reflect the range of essential services and operators that are critical for the downstream gas and electricity system of the future.

For this reason, we propose a review of NIS applicability to DGE, delivered through a review of the essential services covered by the current regulatory framework and associated threshold requirements, to determine whether they remain fit for purpose. In parallel to this consultation, the National Energy System Operator (NESO) will leverage its unique system-wide insight and expertise to provide independent advice to Ofgem and DESNZ on the essential services that should be captured under the regulatory framework based on who plays a critical role in the system, as well as advising on appropriate thresholds.

NESO is responsible for managing and planning Great Britain's electricity and gas networks, operating the electricity system and creating insights and recommendations for the future whole energy system. Following enactment of the Energy Act 2023, NESO is now a public body and key government partner with duties related to energy and security resilience.

[17] Regulation 8(1) of the NIS Regulations
[18] Regulation 8(3) of the NIS Regulations

Therefore, Ofgem and DESNZ have assessed that NESO is best placed to provide independent advice to Government.

Table 1 outlines the DGE essential services that are currently in scope of the NIS regulations in Great Britain, and the thresholds that operators delivering these services need to meet to be deemed designated as Operators of Essential Services.

Table 1: DGE essential services and thresholds under the NIS Regulations[19]

	Electricity	Gas (Downstream)
Generation*	≥ 2 GW (cumulative)	N/A
Transmission**	> 250,000 final customers	> 250,000 final customers
Offshore Transmission***	≥ 2 GW (cumulative)	N/A
Distribution	> 250,000 final customers	> 250,000 final customers
Interconnectors	≥ 1 GW	> 20M m^3 gas/ day
Supply	> 250,000 final customers	> 250,000 final customers
Load Control****	≥ 300 MW	N/A

**Excludes nuclear electricity generators and generators that are not connected to a transmission system. The generation capacity of all affiliated undertakings is cumulated and assessed against the threshold.*

*** Excludes transmission systems that hold an offshore transmission licence or interconnector licence*

**** The transmission capacity of all affiliated undertakings is cumulated and assessed against the threshold.*

***** Not yet effective but included in the specific NIS amendments within the CSRB. NIS applicability review does not intend to consider load control given this is a recent addition to the CSRB. It will focus on the thresholds and essential services set in the NIS regulations 2018.*

The energy system has changed considerably since the NIS Regulations came into force in 2018, which necessitates a review of our assessment of what is critical for system stability. The essential services defined under the NIS Regulations for DGE cover most of Ofgem's licensed sub-sectors. Where licensed activities were not considered in scope of NIS, this was because the service they provided played an important but non-critical role in the energy system. If this

[19] The Network and Information Systems Regulations 2018- Schedule 2

is still the case after our review, these will still not be brought into scope of the NIS Regulations. If however the criticality of certain services has changed, our review may result in bringing more Ofgem licensees into scope of NIS.

It is also worth noting that there are sectors that are not licensed by Ofgem but may play a critical role in DGE. These sectors may also be considered for inclusion within the scope of the NIS Regulations based on the risks they pose.

Reviewed NIS applicability expected impact

Organisations in scope of the NIS Regulations need to take steps that are appropriate to their operations to effectively reduce their risk.

There would be a financial impact on Government and on organisations brought into scope. Organisations brought into scope may need to fund a range of activities related to familiarisation, compliance and administration, and are likely to require additional security spending (e.g. risk profiling, technology costs, and staffing or training costs)[20]. Not all businesses will incur the same costs, as this would be based on their own risks and existing cyber maturity. As an example – and to help illustrate the size of the potential costs – the Cyber Security and Resilience Impact Assessment[21] estimated the impact on large load controllers from revising the scope of the NIS regulations. Total one-off costs per controller are estimated to range between approximately £110,000 to £130,000 (2025 prices), with ongoing annual costs ranging from £180,000 to £210,000 (2025 prices).

The expected financial impact should be weighed against the cost to a business and the impact to the service of a successful cyber breach or attack. It should also be considered in the context of essential improvements to our national security, and the resilience of essential services, in order to protect the day-to-day functioning of economy and society. If Government takes forward this proposal, the detail and impact of changes to be made to the NIS Regulations will be subject to further consultation.

Reviewed NIS Applicability Questions

Alongside advice from NESO, Ofgem and DESNZ wish to gather views from stakeholders to better understand their perception on how the NIS Regulations should evolve, to ensure all services and operators that could pose a significant risk to the DGE system are appropriately captured.

We therefore welcome views on the following questions:

6. **Do you consider that the current thresholds for the DGE essential services already captured by the NIS Regulations (see Table 1) effectively capture operators of essential services? If not, which thresholds should change, why, and in what direction?**

[20] Post-Implementation Review of the Network and Information Systems Regulations 2018
[21] Cyber Security and Resilience (Network and Information Systems) Bill: supporting documents - GOV.UK

7. **Are there any additional DGE services (excluding supply chain, which is being addressed separately) that should be defined as essential services under the NIS Regulations? Please explain your reasoning.**

Please note that that there is a separate workstream looking into expanding cyber regulation coverage to the energy supply chain. This question is aimed at identifying additional DGE services that should be included (rather than their supply chains).

8. **For any additional services you have proposed under question 7, what threshold would you propose that an operator delivering these services would need to exceed, to be subject to the NIS Regulations (e.g. in terms of capacity, number of customers served, business size etc)? Please expand on your reasoning behind any proposed thresholds.**

Section 3: Baseline Requirements

Introduce baseline cyber resilience requirements for all Ofgem licensees

We propose setting a baseline level of cyber resilience across all DGE Ofgem licensees to be implemented via licence condition updates. Current cyber resilience requirements across the energy sector only apply to operators in scope of the NIS Regulations. However, the shift towards a decentralised, more distributed energy system, means supply resilience will depend on an increasing number of smaller organisations that are unregulated for cyber resilience.

Our proposal for baseline cyber resilience requirements for all Ofgem licensees is intended to be low burden for businesses, and to protect against the most common cyber-attacks by 'doing the basics right'.

Baseline cyber resilience requirements are not intended to represent a final target level of cyber resilience. Instead, they should be regarded as a starting point of baseline cyber hygiene which licensees should aim to exceed based on their individual risk assessments to protect their business and service. The intention is for baseline requirements to foster a positive and comprehensive culture of cyber resilience across the sector, by establishing a starting point that organisations can build on to suit their specific needs.

Ofgem and DESNZ believe it is important to put baseline cyber resilience requirements on a formal footing to ensure consistent baseline adoption across the sector as it evolves and transforms to achieve net zero ambitions.

Establishing a baseline level of cyber security, reduces the risk of opportunistic attacks and strengthens the overall resilience of both businesses and the services they provide.

To provide clear expectations for all licensees, the following **principles for baseline requirements** are proposed:

- They should provide protection against the most common cyber attacks
- They should be low burden for organisations to implement

- They should be a starting point, not a final target. Licensees should build on these requirements based on their business-specific context and individual risk assessment
- They should be independently assured to verify their effectiveness
- They should be shaped in close collaboration with NCSC
- They should be delivered through licences and be applicable to all Ofgem licensees

The Ofgem and DESNZ initial proposal is to use the sector-agnostic Cyber Essentials[22] scheme as a starting point for these baseline cyber resilience requirements. This would have a broad application to all network and information systems in use by the licensees, subject to potential limitations on including operational technology networks.

Cyber Essentials is a government owned scheme, a partnership between DSIT and NCSC, and delivered through IASME (Information Assurance for Small and Medium Enterprises)[23]. It helps organisations defend themselves against the most common cyber threats, via two levels of certification:

- Cyber Essentials (CE) certification: The basic verified self-assessment option
- Cyber Essentials Plus (CE+) certification: Independent technical verification is carried out by the Certification Body

Both levels focus on the same five technical control families that are listed below but differ in the level of assurance required for certification:

- Firewalls and Internet Gateways
- Secure Configuration
- User Access Controls
- Malware Protection
- Patch Management

Though Cyber Essentials has limitations (discussed below) and should be used as a starting point for licensees to build upon, it also has a proven positive impact on organisations of all sizes, ranging from effective vulnerability mitigation and increased risk awareness to the stimulation of wider cyber security practices and the strengthening of assurance mechanisms. Organisations that are certified are 92% less likely to make a cyber insurance claim[24]. A case study from St James' Place saw an 80% reduction in cyber security incidents after implementing Cyber Essentials Plus[25]. The positive impact of the Cyber Essentials scheme goes beyond the protection offered by its five technical controls, as it has been proven that it introduces a wider culture shift in how cyber resilience is viewed within an organisation[26].

[22] Cyber Essentials - NCSC.GOV.UK
[23] Cyber Essentials - IASME
[24] Cyber Essentials management information - GOV.UK
[25] St.James's Place mandates Cyber Essentials Plus across its internal supply chain - IASME - Home
[26] Cyber Essentials impact evaluation - GOV.UK

We are expecting that several Ofgem licensees already implement most of the controls within the Cyber Essentials scheme and would therefore get the most value from Cyber Essentials Plus. This approach would allow Ofgem licensees to test and verify the controls they have implemented, while also giving the greatest assurance to Ofgem and DESNZ on a licensee's cyber resilience.

Though the benefits of the Cyber Essentials scheme are extensive and proven, there are also some significant nuances to consider. The Cyber Essentials scheme is primarily suitable for Information Technology (IT). Many operators in DGE rely on Operational Technology (OT) systems to deliver their services. These include industrial control systems that interact with the physical world (like Supervisory Control and Data Acquisition systems, Programmable Logic Devices, Human Machine Interfaces, Remote Telemetry Units, etc). It may be possible to apply Cyber Essentials controls to OT systems on a case-by-case basis, but their application can be challenging – and in certain circumstances unsuitable.

Additionally, mature cyber resilience requires the implementation of controls across the people, process and technology areas of an organisation. The Cyber Essentials scheme controls are focused on technical measures and may not drive increased maturity in other areas like organisational governance, personnel security, supply chain resilience, response & recovery processes, or other non-technical aspects of cyber resilience.

In the context of DGE, baseline requirements could use the existing five technical control families of the Cyber Essential scheme, or a hybrid scheme could be created with additional controls tailored to the specific needs and risks of Ofgem licensees. We welcome feedback on whether the Cyber Essentials technical controls should be used as they are or adjusted to better reflect the security needs of Ofgem licensees.

Ofgem and DESNZ can see trade-offs in both approaches. Using the Cyber Essentials controls as they are, means that Ofgem licensees can leverage an established, proven, cost-effective scheme which has an extensive pool of assessors. This would allow baseline requirements to be rolled out relatively quickly. Creating additional controls to supplement the existing ones, would necessitate the establishment of a hybrid scheme. This could be more tailored to the needs of Ofgem licensees, therefore providing deeper resilience and assurance, but it would be more complex to develop and implement and there would need to be a re-evaluation of required assessor competency for any future scheme, which may limit the existing pool of assessors.

Supplementary principles / controls to expand scope / make measures more specific to Ofgem licensees could include:

- Separation between IT and OT systems
- Risk assessments
- Organisational policies and training
- Supply chain security
- Response & recovery processes

Baseline requirements expected impact

It is expected that the impact on licensees from baseline requirements will be low. Ofgem currently regulates just over 1,400 licensed operators across the different licensed areas[27]. We anticipate that many Ofgem licensees will already be implementing measures that meet or exceed any future baseline requirements. This is also supported by early evidence through our pre-consultation engagement. For these operators, the impact would be low and limited to demonstrating the effectiveness of practices they already implement. This consultation will gather further evidence to inform our understanding of the costs and impacts of cyber incidents and control implementation across the Ofgem licensees' landscape.

We anticipate that there will be some Ofgem licensees whose security practices may need to be improved to meet baseline requirements. We anticipate the impact on them to also be low compared to the benefit they would stand to gain. If we take Cyber Essentials as a basis for the expected costs of implementing a baseline level of cyber hygiene, the Government's 2023 process evaluation found that the average costs for organisations to become Cyber Essentials (CE/CE+) certified (including the costs of implementing controls) were estimated as follows by business size band: micro (£1,894), small (£4,741), medium (£6,267), and large (£31,459)[28]. It is important to note that these figures are not sector specific and are used to provide an indication. Through this consultation, we seek feedback to get more energy-specific estimates on the costs of Cyber Essentials certification.

The potential return on that investment needs to consider both the financial and non-financial consequences of a cyber-attack upon an organisation – which are difficult to quantify. Recent DSIT-commissioned research from KPMG[29] estimated that the average cost of a significant cyber-attack for a UK organisation is just below £195,000. For utilities specifically, this is higher, at over £210,000[30]. The cost varies based on organisation size, ranging from £93,665 for micro businesses in the utilities space to £436,443 for large ones. With the DSIT cyber breaches 2025 survey stating that just over 4 in 10 (43%) of businesses reported having experienced any kind of cyber security breach or attack in the last 12 months[31], we expect that the benefits of baseline cyber hygiene will outweigh the costs.

Using Cyber Essentials again as an example of baseline cyber resilience, the Government's 2024 impact evaluation found that Cyber Essentials benefits go beyond the protection provided through the scheme's five technical controls, with the certification stimulating wider actions, good practice and behaviours, improving organisations' awareness and understanding of the cyber risk environment. Subject to certain conditions, Cyber Essentials also offers

[27] Home Page - Ofgem Public Register
[28] Cyber_Essentials_Process_Evaluation.pdf
[29] Economic_modelling_of_sector_specific_costings_of_cyber_attacks.pdf
[30] Definition of utilities for the purposes of this figure: North American Industry Classification System (NAICS) U.S. Census Bureau We recognise that these figures are based on US data and are not sector specific, as they combine both the water and energy sector for utilities. However, we consider them to be adequate to indicate a need for change. We will use this consultation as means for gathering UK sector specific information for energy.
[31] Cyber security breaches survey 2025 - GOV.UK

organisations with turnovers of less than £20m free cyber insurance, including incident response coverage.

When considering the expected impact of baseline requirements, it is also important to consider the counterfactual – the impact in the absence of the proposed measure. Lack of activity in this space could leave a number of licensees outside the scope of cyber resilience requirements, therefore failing to address the cyber risk to both their businesses and the services they provide. Specifically for the sectors that are actively growing to meet net-zero ambitions, the lack of baseline requirements would also be a missed opportunity to embed basic security in the design stage, therefore risking a security debt that would need to be retrospectively addressed at a higher cost.

Baseline Requirements Questions

Ofgem and DESNZ want to gather additional evidence to inform our collaborative work with NCSC to shape baseline cyber resilience requirements for all Ofgem licensees. This evidence will inform the development of a detailed proposal for baseline requirements.

A subset of Ofgem licensees also fall under the scope of NIS and are therefore already subject to NIS cyber resilience requirements. NIS requirements only apply to network and information systems on which the essential service relies or that are used for the provision of the essential service. Therefore, Ofgem licensees that are subject to NIS are not required to protect their full network and information system estate and therefore ancillary, supporting and back-end systems can fall outside the scope of cyber resilience requirements and would benefit from baseline requirements.

We are interested in hearing both from Ofgem licensees who are and those who are not currently subject to the NIS Regulations. Where questions in this section target a specific audience, this is specified in the questions themselves. If a target audience is not specified, the question is applicable to all Ofgem licensees.

In addition, we want to hear from stakeholders including but not limited to academia, research bodies and industry bodies who can provide a substantiated opinion due to their experience with Ofgem licensees.

9. **What are your views on the proposed principles for baseline requirements? Please explain the reasoning for your response.**

10. **What are your views on our proposal to use the Cyber Essentials scheme (CE/CE+) as a basis for shaping baseline cyber resilience requirements for all Ofgem licensees? Do you think the existing five control families are adequate, or would you advise to go beyond them and develop a bespoke scheme that is based on Cyber Essentials but also includes additional controls specific to Ofgem licensees? Please explain.**

11. **If in question 10 you were in favour of a bespoke scheme, what additional principles or controls do you consider most important to shape appropriate baseline requirements for all Ofgem licensees?**

12. **Are there any alternative schemes or standards that you might suggest as a basis for shaping baseline cyber resilience requirements? If yes, please elaborate on what these are and why you think they would be suitable.**

13. **For Ofgem licensees that currently hold or have previously held Cyber Essentials or Cyber Essentials Plus certifications, what was the average total cost (including certification and control implementation)?**

14. **For Ofgem licensees that currently hold or have previously held Cyber Essentials or Cyber Essentials Plus certifications, did you face any barriers to achieving certification? Please expand.**

15. **If you do not hold a Cyber Essentials or Cyber Essentials Plus certification, have you attempted to and what were the financial and/or practical barriers to achieving this?**

Due to information sensitivity considerations, we will not publish summaries of consultees' responses to the following questions or a Government position in the Government's consultation response.

16. **If you are an Ofgem licensee not currently captured by the NIS Regulations, are you proactively implementing cyber resilience measures across people, processes and technology to protect your business and services against cyber-attacks?**

17. **If you are an Ofgem licensees not captured by the NIS Regulations, do you currently hold cyber certifications (e.g. Cyber Essentials, Cyber Essentials Plus, ISO 27001 or other)? If yes, what certifications and is their scope wide enough to protect all your network and information systems?**

18. **If you are an Ofgem licensee not currently captured by the NIS Regulations, have you experienced impacts from cyber incident(s) in the last 24 months? If so, what was the impact on the business or service (including costs where figures or estimates are available) and what were the most common types of cyber incidents experienced (e.g. ransomware, phishing, supply chain attacks etc)?**

19. **If you are an Ofgem licensee captured by the NIS Regulations, do you currently hold cyber certifications (e.g. Cyber Essentials, Cyber Essentials Plus, ISO 27001 or other) for the network and information systems that are not within the scope of NIS? If yes, what certifications and is their scope wide enough to protect all your systems outside the scope of NIS?**

20. **If you are an Ofgem licensee currently captured by the NIS Regulations, have you experienced impacts from cyber incident(s) in the last 24 months (please consider all impacts, not just the ones affecting the essential service)? If so, what was the impact on the business or service (including costs where figures or estimates are available) and what were the most common types of cyber incidents experienced (e.g. ransomware, phishing, supply chain attacks etc)?**

Section 4: Demographic Questions

21. **Are you responding as an individual or on behalf of an organisation?**

a. Individual

b. Organisation

22. If an individual, what is your interest in this space?

a. [include text box here]

23. If an individual, which of the following statements best describes your role?

a. Cyber Security Professional

b. Operations / Engineering

c. Policy / Regulation

d. Legal / Compliance

e. Executive / Senior Leadership

f. Other [include text box]

24. If an organisation, what is your organisation's name?

a. [include text box]

25. If an organisation, what type of organisation do you represent?

a. Ofgem Licensee

b. Government

c. Academia

d. Trade Body

e. Developer

f. Original Equipment Manufacturers (OEMs) or Distributors

g. Load Controller

h. Other [include open textbox]

26. If an organisation, how many people work for your organisation? If unsure, please provide your best estimate.

a. Under 10

b. 10-49

c. 50-249

d. 250-499

e. Over 499

f. Not sure

27. If you are licensed by Ofgem, is your organisation an Operator of Essential Services under the NIS Regulations?

a. Yes

b. No

28. If you are licensed by Ofgem, what type(s) of licence(s) does your organisation hold? [allow ability to select multiple responses]

a. Gas transporter (including National Transmission System - NTS)

b. Independent gas transporter

c. Gas supply (domestic & non-domestic)

d. Gas supply (non-domestic only)

e. Gas supplier (Non-Transporter / Private Network)

f. Gas shipper

g. Gas interconnector

h. Electricity generation

i. Electricity transmission (onshore)

j. Electricity transmission (offshore)

k. Electricity distribution

l. Independent electricity distribution

m. Electricity supply (domestic / non-domestic)

n. Electricity supply (non-domestic only)

o. Electricity interconnector

p. System operator

q. Gas System Planner

r. Smart meter communications

s. Carbon dioxide transport and storage

29. If you hold an electricity generation licence, what types of assets does your organisation manage? [allow ability to select multiple responses]

a. Offshore Wind Generation

b. Onshore Wind Generation

c. Solar Generation

d. Battery Energy Storage Systems (BESS)

e. Long Duration Energy Storage (excluding BESS)

f. Non-renewable Generation

g. Other – please specify [Text box here]

Consultation Questions

Section 1: Proposed Approach

1. Is there a need to expand the scope of our cyber oversight and assurance to cover more DGE operators? Please provide further detail on why.

2. If you answered yes to question 1, what are your views on our proposal to expand the scope of our cyber oversight and assurance to cover more DGE operators by: (a) reviewing who NIS applies to and ensuring the most critical DGE operators for the increasingly distributed and digitalised energy system fall within its scope and (b) introducing baseline cyber resilience requirements for all Ofgem licensees?

3. Are there any alternative approaches we should consider on how to expand the scope of our cyber oversight and assurance and build resilience across the sector, whilst maintaining strong cyber security measures for critical operators? Please explain your reasoning.

4. Do you think there is a need for intermediate cyber requirements (above baseline but below NIS) in DGE? If so, do you think these should be considered in a staged approach (implementing baseline requirements for all Ofgem licensees and reviewing NIS applicability first before proceeding to scoping intermediate requirements)? Please explain your reasoning.

5. If you think there is a need for intermediate requirements, what risks should they look to address and who should they target?

Section 2: Reviewed NIS Applicability

6. Do you consider that the current thresholds for the DGE essential services already captured by the NIS Regulations (see Table 1) effectively capture operators of essential services? If not, which thresholds should change, why, and in what direction?

7. Are there any additional DGE services (excluding supply chain, which is being addressed separately) that should be defined as essential services under the NIS Regulations? Please explain your reasoning.

8. For any additional services you have proposed under question 7, what threshold would you propose that an operator delivering these services would need to exceed, to be subject to the NIS Regulations (e.g. in terms of capacity, number of customers served, business size etc)? Please expand on your reasoning behind any proposed thresholds.

Section 3: Baseline Requirements

9. What are your views on the proposed principles for baseline requirements? Please explain the reasoning for your response.

10. What are your views on our proposal to use the Cyber Essentials scheme (CE/CE+) as a basis for shaping baseline cyber resilience requirements for all Ofgem licensees? Do you think the existing five control families are adequate, or would you advise to go beyond them and develop a bespoke scheme that is based on Cyber Essentials but also includes additional controls specific to Ofgem licensees? Please explain.

11. If in question 10 you were in favour of a bespoke scheme, what additional principles or controls do you consider most important to shape appropriate baseline requirements for all Ofgem licensees?

12. Are there any alternative schemes or standards that you might suggest as a basis for shaping baseline cyber resilience requirements? If yes, please elaborate on what these are and why you think they would be suitable.

13. For Ofgem licensees that currently hold or have previously held Cyber Essentials or Cyber Essentials Plus certifications, what was the average total cost (including certification and control implementation)?

14. For Ofgem licensees that currently hold or have previously held Cyber Essentials or Cyber Essentials Plus, did you face any barriers to achieving certification? Please expand.

15. If you are an Ofgem licensees not captured by the NIS Regulations, do you currently hold cyber certifications (e.g. Cyber Essentials, Cyber Essentials Plus, ISO 27001 or other)? If yes, what certifications and is their scope wide enough to protect all your network and information systems?

Due to information sensitivity considerations, we will not publish summaries of consultees' responses to the following questions or a Government position in the Government's consultation response.

16. If you are an Ofgem licensee not currently captured by the NIS Regulations, are you proactively implementing cyber resilience measures across people, processes and technology to protect your business and services against cyber-attacks?

17. If you are an Ofgem licensees not captured by the NIS Regulations, do you currently hold cyber certifications (e.g. Cyber Essentials, Cyber Essentials Plus, ISO 27001 or other)? If yes, what certifications and is their scope wide enough to protect all your network and information systems?

18. If you are an Ofgem licensee not currently captured by the NIS Regulations, have you experienced impacts from cyber incident(s) in the last 24 months? If so, what was the impact on the business or service (including costs where figures or estimates are available) and what were the most common types of cyber incidents experienced (e.g. ransomware, phishing, supply chain attacks etc)?

19. If you are an Ofgem licensee captured by the NIS Regulations, do you currently hold cyber certifications (e.g. Cyber Essentials, Cyber Essentials Plus, ISO 27001 or other) for the network and information systems that are not within the scope of NIS? If yes, what certifications and is their scope wide enough to protect all your systems outside the scope of NIS?

20. If you are an Ofgem licensee currently captured by the NIS Regulations, have you experienced impacts from cyber incident(s) in the last 24 months (please consider all impacts, not just the ones affecting the essential service)? If so, what was the impact on the business or service (including costs where figures or estimates are available) and what were the most common types of cyber incidents experienced (e.g. ransomware, phishing, supply chain attacks etc)?

Section 4: Demographic Questions

21. Are you responding as an individual or on behalf of an organisation?

    a. Individual
    b. Organisation

22. If an individual, what is your interest in this space?

    a. [include text box here]

23. If an individual, which of the following statements best describes your role?

    a. Cyber Security Professional
    b. Operations / Engineering
    c. Policy / Regulation

d. Legal / Compliance
e. Executive / Senior Leadership
f. Other [include text box]

24. If an organisation, what is your organisation's name?

a. [include text box]

25. If an organisation, what type of organisation do you represent?

a. Ofgem Licensee
b. Government
c. Academia
d. Trade Body
e. Developer
f. Original Equipment Manufacturers (OEMs) or Distributors
g. Load Controller
h. Other [include open textbox]

26. If an organisation, how many people work for your organisation? If unsure, please provide your best estimate.

a. Under 10
b. 10-49
c. 50-249
d. 250-499
e. Not sure

27. If you are licensed by Ofgem, is your organisation an Operator of Essential Services under the NIS Regulations?

a. Yes
b. No

28. If you are licensed by Ofgem, what type(s) of licence(s) does your organisation hold? [allow ability to select multiple responses]

a. Gas transporter (including National Transmission System - NTS)
b. Independent gas transporter
c. Gas supply (domestic & non-domestic)
d. Gas supply (non-domestic only)
e. Gas supplier (Non-Transporter / Private Network)
f. Gas shipper
g. Gas interconnector
h. Electricity generation
i. Electricity transmission (onshore)
j. Electricity transmission (offshore)
k. Electricity distribution
l. Independent electricity distribution
m. Electricity supply (domestic / non-domestic)
n. Electricity supply (non-domestic only)
o. Electricity interconnector
p. System operator
q. Gas System Planner

r. Smart meter communications
s. Carbon dioxide transport and storage

29. If you hold an electricity generation licence, what types of assets does your organisation manage? [allow ability to select multiple responses]

a. Offshore Wind Generation
b. Onshore Wind Generation
c. Solar Generation
d. Battery Energy Storage Systems (BESS)
e. Long Duration Energy Storage (excluding BESS)
f. Non-renewable Generation
g. Other – please specify [Text box here]

Glossary

Acronym	Term
AI	Artificial Intelligence
BESS	Battery Energy Storage Systems
CAF	Cyber Assessment Framework
CE	Cyber Essentials
CE+	Cyber Essentials Plus
CSRB	Cyber Security Resilience (Network and Information Systems) Bill
DESNZ	The Department for Energy Security and Net Zero
DGE	Downstream Gas and Electricity
DSIT	Department for Science Innovation and Technology
IASME	Information Assurance for Small and Medium Enterprises
IT	Information Technology
NCSC	National Cyber Security Centre
NESO	National Energy System Operator
NIS Regulations	Network Information Systems Regulations
NTS	National Transmission System
OES	Operators of Essential Services
Ofgem	The Office for Gas and Electricity Markets
OT	Operational Technology

This publication is available from: www.gov.uk/government/consultations/whole-energy-cyber-resilience-requirements-reshaping-cyber-regulation-in-downstream-gas-and-electricity

Any enquiries regarding this publication should be sent to us at:
cyber.policy@energysecurity.gov.uk or CyberStrategy@ofgem.gov.uk

If you need a version of this document in a more accessible format, please email alt.formats@energysecurity.gov.uk. Please tell us what format you need. It will help us if you say what assistive technology you use.