ofgem
Making a positive difference for energy consumers

UK Government

Reshaping Cyber Regulation in Downstream Gas and Electricity

Government Response

Department for Energy Security and Net Zero (2026)

Contents

Ministerial foreword

A secure and resilient energy system underpins the country's national security, economic stability, and everyday life. As our energy system rapidly becomes increasingly digital, decentralised and interconnected, cyber threats are evolving in scale and sophistication. Stronger, more adaptive regulation is essential. Cyber security should be a fundamental requirement for anyone operating in our energy system.

The December 2025 attack on the Polish energy system demonstrated that adversaries see energy as an attractive target. Our approach needs to keep pace with the current threat landscape. Recent government publications[1], emphasise government's commitment to securing our country and energy system against cyber threats.

Our work to reshape cyber regulation is directly linked to this commitment. The recent consultation provided valuable insights from industry and other stakeholders. We were pleased to see broad support for the proposals, which reflect our shared dedication to maintain a secure and resilient energy system.

Our proposals are centred around two fundamental reform needs. Firstly, considering the energy system and technology transformation, there is a need to undertake a thorough review and reevaluate who are the most critical organisations in the Downstream Gas and Electricity (DGE) subsectors. DESNZ will take this work forward and use NESO's energy system advice, alongside feedback from this consultation to shape NIS applicability review proposals.

DESNZ would then engage with the Department for Culture, Media and Sport (DCMS) on leveraging the powers that will become available through the Cyber Security and Resilience Bill (CSRB) to amend the scope of the Network and Information System (NIS) Regulations 2018 and ensure it reflects the needs of the transforming energy system. The CSRB represents a major step change in our ability to protect vital public services and critical infrastructure and is a key enabler for the NIS applicability review proposed in the consultation and is currently in passage through the House of Lords.

Secondly, considering the interconnectedness of the energy system, the evolving threat landscape and the absence of cyber resilience requirements across a big part of Ofgem-licensed organisations, there is a need to reshape how we conduct cyber regulation and ensure that all Ofgem licensees have a consistent baseline level of cyber resilience. This is aimed at protecting both their business, and the services they provide to consumers. Ofgem will take this work forward and will consult the National Cyber Security Centre (NCSC) and the industry to shape and implement appropriate baseline cyber resilience requirements.

These proposals sit alongside wider changes to cyber regulation, including the CSRB, which will result in changes for regulated organisations and the ongoing negotiations for an Electricity Agreement for the UK to rejoin the EU's Internal Electricity Market (which would be

[1] Energy sector cyber security strategy - GOV.UK

implemented using powers in the European Partnership Bill). The latter has the potential to impact UK cyber regulation for organisations involved in cross-border electricity flows. We will be cognisant of wider cyber reform implications when shaping the work under this government response. We will work in lockstep with DCMS and NCSC to streamline regulatory requirements and ensure our framework is clear.

This consultation response marks a decisive step forward in strengthening the resilience of the UK's downstream gas and electricity system. We will continue to work closely with industry and partners as we implement these reforms, ensuring our approach remains effective, and responsive to the evolving threat landscape.

Minister Shanks

Minister of State for Energy

Tim Jarvis

Chief Executive Officer, Ofgem

1 General information

1.1 Context to this consultation

This document sets out the government's response to the Reshaping Cyber Regulation in Downstream Gas and Electricity consultation[2], a joint consultation by the Department of Energy Security and Net Zero (DESNZ) and Ofgem, which was published on 27 March 2026 and closed on 22 May 2026. It provides a summary of responses to each question in the consultation, and our government response on each topic.

We received 49 responses to this consultation. A breakdown of who responded can be found in the demographics section below.

Contact details

For questions related to policy decisions or this document please contact: cyber.policy@energysecurity.gov.uk and CyberStrategy@ofgem.gov.uk

[2] Whole energy cyber resilience requirements: reshaping cyber regulation in downstream gas and electricity - GOV.UK

2 Consultation responses and government response

This section outlines the main themes arising from stakeholders' responses that have been shared on a non confidential basis. Due to information sensitivity considerations, we stated we would not publish summaries of consultees' responses or a government position to questions related to the voluntary implementation of cyber resilience measures and certifications, and to the prevalence and impact of cyber incidents in the sector (questions 16 to 20 in the consultation). The responses to these questions will still be considered when developing future policy. Ofgem and DESNZ will reconsult with the sector once more detailed policy options have been developed.

2.1 Response Demographics

We received a total of **49 responses** to the consultation.

- **3** responses from **individuals**
- **46** responses from **organisations**

All the individuals had a background in IT or cyber security.

Out of the **46 organisations** that responded:

- **30** were **Ofgem licensees**
- **16** were **not licensed by Ofgem**

Out of the 16 organisations that were **not licensed by Ofgem**:

- **10** were a service or tool provider related to cyber security
- **1** was an Original Equipment Manufacturer
- **5** were active in other areas (code bodies, trade bodies, professional bodies, government or academia)

Out of the **30** organisations that were **licensed by Ofgem:**

In terms of **business size**:

- **20** respondents reported having >499 employees
- **1** respondent reported having 250-499 employees
- **6** respondents reported having 50-249 employees
- **2** respondents reported having 10-49 employees
- **1** respondent did not provide an answer

In terms of **Network and Information Systems (NIS) Regulations Operator of Essential service (OES) status**:

- **20** respondents reported that they were NIS OES
- **8** respondents reported that they were not NIS OES
- **1** respondent was unsure
- **1** respondent did not answer the question

In terms of **types of licenses held** by licensees that responded (please note a respondent can hold multiple licence types)

- **15** reported holding electricity generation licences
- **10** reported holding electricity distribution licences (including independent distribution)
- **9** reported holding gas shipping licences

- **8** reported holding gas supply licences
- **8** reported holding electricity supply licences
- Other types of licences were also represented in lower numbers

In terms of **types of generation assets managed by licensees who reported holding electricity generation licenses** (please note an electricity generation licence holder may manage multiple types of generation assets)

- **9** reported managing wind generation assets (onshore or offshore)
- **7** reported managing Battery Energy Storage Systems (BESS) assets
- **7** reported managing non-renewable generation assets
- **5** reported managing solar generation assets
- **1** reported managing Long Duration Energy Storage (excluding BESS) assets
- **2** reported managing other electricity generation assets
- **1** did not respond

Please note that we will not be sharing the names of individuals or organisations that responded, to avoid the public identification of organisations that are classed as Operators of Essential Services under NIS. We consider the demographic breakdown provided above to be sufficient for the purpose of this government response.

2.2 The proposals

2.2.1 Proposed Approach

We sought views on expanding cyber oversight and assurance by firstly reviewing the scope of the NIS regulations and secondly introducing baseline requirements for all Ofgem licensees. We also invited feedback on potential alternative approaches to strengthening resilience, including whether intermediate requirements (above baseline requirements but below NIS) are needed and what they should address or target.

2.2.1.1 Question analysis

Q1. Is there a need to expand the scope of our cyber oversight and assurance to cover more downstream gas and electricity (DGE) operators? Please provide further detail on why.

Table 1 below outlines respondents' position on Question 1.

Table 1: Question 1 response breakdown

Response	Nr of responses	% of responses
Agree with the need	35	~72%
Cautiously agree with the need	9	~18%
Disagree with the need	1	~2%
No response	4	~8%
Totals	**49**	**100%**

As can be seen in Table 1, 44 out of 49 respondents broadly agreed that there is a need to expand the scope of cyber oversight and assurance in Downstream Gas and Electricity to cover more operators.

The following themes were cited as reasons for agreement:

- The energy sector transformation (digitalisation, interconnectedness, decentralisation)
- Smaller, distributed operators' potential to affect the system due to cascading vulnerabilities and systemic risks
- Complex and interconnected supply chains
- An evolving threat landscape

Out of the 44 that agreed, 9 were cautious in their agreement. Most of the respondents that cautiously agreed were organisations licensed by Ofgem (8), with 5 of these 8 also being OES under the NIS Regulations 2018. The remaining one organisation that cautiously agreed was a

trade body. These respondents were supportive in principle but encouraged DESNZ and Ofgem to:

- Make sure the approach is proportionate and risk-based, avoiding one-size-fits-all solutions
- Consider impact and criticality which may require approaches beyond threshold- setting
- Avoid regulatory burden and requirement duplication
- Ensure regulators are appropriately resourced for any expanded role

The one respondent who disagreed (an Ofgem licensee) expressed a preference for non-regulatory approaches and queried whether an expansion of regulation would be in line with the policy intent of the NIS Regulations. This respondent also outlined concerns on burden, both on the industry to implement any new requirement and the regulator who oversees them.

Q2. 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?

Table 2 below outlines respondents' position on Question 2 (a).

Table 2: Question 2 (a) response breakdown

Response	Nr of responses	% of responses
Agree with a review of NIS	33	~67%
Cautiously agree with a review of NIS	11	~23%
Disagree with a review of NIS	1	~2%
No response	4	~8%
Totals	**49**	**100%**

There was broad support among respondents for expanding cyber oversight and assurance across DGE, specifically by reviewing which operators should be brought into scope of NIS Regulations. In total 43 respondents broadly agreed (see Table 2). Of these, 29 were Ofgem licensees, over half of whom (19) were NIS OES.

Commonly cited reasons (as aligned with Question 1) included:

- The energy sector transformation (digitalisation, interconnectedness, decentralisation)
- Smaller, distributed operators' potential to affect the system due to cascading vulnerabilities and systemic risks
- Complex and interconnected supply chains

- An evolving threat landscape

Of the 43 respondents that agreed, 11 expressed cautious agreement. Their support was contingent on DESNZ and Ofgem ensuring the following, noting alignment with the reasons set out in response to Question 1:

- The approach is proportionate and risk-based, avoiding one size fits all solutions
- Considers impact and criticality which may require approaches beyond threshold setting
- Avoids regulatory burden and a duplication of existing regulation
- Ensures the regulator has sufficient resource and capability to manage its expanded scope.

One respondent (an Ofgem licensee) opposed extending NIS to their subsector through a wider review of NIS applicability. They argued that the small scale localised nature of their operations limits potential impact, making inclusion under NIS disproportionate, therefore the requirements should not be applicable.

Table 3 below outlines respondents' position on Question 2 (b).

Table 3: Question 2 (b) response breakdown

Response	Nr of responses	% of responses
Agree with the introduction of baseline requirements	28	~57%
Cautiously agree with the introduction of baseline requirements	14	~29%
Disagree with the introduction of baseline requirements	1	~2%
No response	6	~12%
Totals	**49**	**100%**

Table 3 sets out overall support for expanding the scope of cyber oversight and assurance, through the introduction of baseline requirements. A total of 42 respondents either agreed or cautiously agreed. This included 27 Ofgem licensees, 18 of whom were NIS OES.

Common drivers underpinning this support included:

- The need to improve consistency, introduce standardisation and raise the cyber maturity of the sector.
- The implications of energy sector transformation (digitalisation, interconnectedness, decentralisation)
- The importance of addressing supply chain risk

  One respondent disagreed but did not provide further explanation.

Q3. 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.

Table 4 below outlines respondents' position on Question 3.

Table 4: Question 3 response breakdown

Response	Nr of responses	% of responses
Suggested alternative approaches while also having expressed agreement with proposal	34	~70%
Suggested alternative approaches but expressed disagreement with the proposal	3	~6%
No alternative approaches proposed while also having expressed agreement with our proposal	10	~20%
No response	2	~4%
Totals	**49**	**100%**

When asked whether there were any alternative approaches that DESNZ and Ofgem should consider for expanding cyber oversight and assurance, 37 proposed alternative approaches, 10 respondents did not propose alternative approaches, and 2 did not respond.

Of those that suggested alternative approaches, 34 had previously expressed agreement with our proposed approach in previous questions. Therefore, their suggestions intended to build on our proposals rather than replace them. 20 of these were Ofgem licensees and 14 non-licensees, including cyber security providers or consultancies.

Suggested approaches and considerations included:

- Ensuring the approach is proportionate and risk-based, avoiding one size fits all solutions
- To take account of impact and criticality which may require approaches beyond threshold setting
- Consider a tiered approach
- Aligning with existing standards to avoid regulatory burden and duplication
- To consider funding and resourcing for smaller operators

Although this topic is addressed further down (see Question 11 which explored additional controls Ofgem and DESNZ should consider for baseline requirements), some respondents

also used this question as an opportunity to suggest specific themes for additional controls. Commonly cited controls included:

- Software management, cloud services and remote access management
- Supply chain visibility
- IT / OT segregation

A small number of respondents (3) that suggested alternative approaches, expressed disagreement with our proposed approach, preferring the use of existing frameworks such as the CAF or user security assessment required under the Smart Energy Code (SEC).

Q4 & Q5: Intermediate Requirements

Q4. 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.

Q5. If you think there is a need for intermediate requirements, what risks should they look to address and who should they target?

Questions 4 and 5 have been grouped together as they both cover intermediate requirements. Additionally, Question 5 was not included on the Citizen's Space portal[3] so less responses were received for this question. 18 respondents answered this question either via email or in their response to question 4.

Table 5 and Table 6 below outline respondents' answers to Question 4.

Table 5: Question 4a response breakdown- need for intermediate requirements

Response	Nr of responses	% of responses
Agree with the need for intermediate cyber requirements	23	~47%
Disagree with the need for intermediate cyber requirements	16	~33%
Unsure if there is a need	6	~12%
No response	4	~8%
Totals	**49**	**100%**

[3] This was due to a technical error but we consider it does not impact overall results as we received sufficient feedback on this topic through Question 4 and email responses.

Table 6: Question 4b response breakdown- staging of intermediate requirements

Response	Nr of responses	% of responses
Agree intermediate requirements should be staged	18	~37%
Disagree, intermediate requirements should not be staged	2	~4%
Unsure whether they should be staged	1	~2%
No response	13	~26%
Did not agree with intermediary requirements	15	~31%
Totals	**49**	**100%**

A higher proportion of respondents (47%) were in favour of intermediate requirements; however, a significant amount (33%) disagreed with the need.

The 23 respondents who agreed were comprised of 12 Ofgem licensees, 7 service providers and 4 other organisations. The 16 who disagreed were 13 Ofgem licensees, 2 service providers and 1 individual.

The most common reasons given for supporting intermediate requirements were to fill the gap between baseline and NIS requirements (14 respondents), to build operational resilience (7 respondents) and to give organisations a clear progression pathway (4 respondents).

The reasons given by those who disagreed with the need to implement intermediate requirements were more varied. The most common reasons given were:

- That the existing/proposed frameworks (baseline and NIS) are sufficient, and additional requirements beyond this would be unnecessary (11 respondents);
- Intermediate requirements would create regulatory complexity and duplication without significant benefit (9 respondents);
- Introducing intermediate requirements could cause significant burden on organisations in scope and delay implementation of baseline requirements (3 respondents);
- There is currently a lack of evidence for needing these requirements (3 respondents); and
- The fixed tiers created by intermediate requirements would be too static for such a dynamic sector (3 respondents).

Of those who agreed and expressed a view, 86% believed that intermediate requirements should be implemented in a staged manner (after baseline requirements have been implemented and NIS applicability has been reviewed).

Of the respondents who supported the staged approach, the primary reasons cited were to allow time for government to understand the implications of baseline requirements and the NIS applicability review and build an evidence base for the need for intermediate requirements (16 respondents) and to reduce the implementation burden on industry (9 respondents).

Of the organisations who supported bringing in intermediate requirements, only 2 respondents (an Ofgem licensee and a cyber-security consultancy firm) disagreed with implementing intermediate requirements in a staged way. The reasons given were to maximise regulatory clarity and urgently address the evolving cyber threat landscape.

Respondents to Question 5 suggested the following categories of risk as priority areas for intermediate requirements:

- Operational technology (OT), remote access and control system compromise risk (8 respondents)
- Interconnectivity and cascading system impact risk (7 respondents)
- Supply chain dependency risk (4 respondents)
- Vulnerability monitoring and incident management risk (3 respondents)
- Risk of lack of proper assurance and verification (3 respondents)

The following categories of organisation were suggested to be in scope of intermediate requirements:

- Organisations which, if compromised, could result in wider disruption, such as those that depend heavily on third parties, are closely linked with other organisations, or bring together control of many smaller energy assets (10 respondents)
- Mid-size organisations who are out of scope of NIS Regulations due to their size but, if compromised, could have a significant customer, operational or system stability impact (8 respondents)
- Supply chain (5 respondents)
- Data sharing infrastructure (4 respondents)
- Multi-party platforms (2 respondents)

2.2.1.2 Government Response

Proposed approach

We welcome the broad support for our proposals and policy direction in reshaping cyber requirements for the DGE sector.

Most respondents agreed with our proposals subject to the requirements being:

- Proportionate
- Risk-based
- Appropriate to the size of the organisation

- Considerate of criticality and material impact
- Not overly burdensome on the regulator
- Avoiding regulatory burden and duplication and
- Having clear direction.

We agree with the need to shape any new or updated requirements carefully around these considerations. Any expansion to requirements will be carried out in close collaboration with key government partners to ensure there is a robust evidence base and technical advice.

Our goal is to design a cyber regime which prevents attacks disrupting our energy system, without placing undue burden on organisations or the regulator.

Baseline requirements

We intend for baseline requirements to ensure a consistent minimum level of resilience across the sector, fostering a strong cyber security culture across organisations of all sizes. Cyber security should be a key consideration for every operator involved in providing gas and electricity services to our country and the continued operation of their organisation. Baseline requirements intend to ensure that no organisation falls behind a minimum standard and that requirements are not unduly onerous, especially for smaller organisations with less cyber security expertise and resource.

Ofgem will use the consultation responses and work with the NCSC to further shape baseline requirements for all Ofgem licensees and outline implementation proposals. We will consult on these with the sector to gather feedback and further refine our approach. The proposals will consider how baseline requirements can complement, not duplicate, existing requirements and offer protection whilst minimising regulatory burden. They will also explore appropriate assurance options and consider roll-out and implementation timelines. This work will be delivered in consultation with DESNZ but will be Ofgem-led, as baseline requirements will be processed via Ofgem licence changes.

NIS applicability review

The NIS Regulations came into force in 2018 to improve the cyber security of companies providing essential services. We want to ensure that the essential service definitions and thresholds for DGE reflect the current and future system, and the risks it faces.

On 12 November 2025 the Cyber Security and Resilience (Network and Information Systems) Bill (CSRB) was introduced to Parliament to tackle the evolving cyber threats faced by the UK. The CSRB includes updates to the NIS Regulations 2018 and will protect more essential and digital services from cyber attacks, enable cyber regulators to be more effective, and provide the Government with the flexibility to respond to new threats in the cyber landscape. This includes the power for the Secretary of State to update the regulatory framework, including bringing more services scope through secondary legislation. These powers will unlock DESNZ and Ofgem's proposals to expand the scope of the NIS Regulations for the DGE sector by providing the regulatory levers required.

The NIS applicability review seeks to ensure that those providing the most critical services to our energy system are captured by the NIS Regulations, to prevent the potential impact of disruption to our essential energy supply. Ofgem and DESNZ will continue to work with the National Energy System Operator (NESO) to assess risks and impacts on the downstream gas and electricity system.

NESO has the statutory duty, set out in section 171 of the Energy Act 2023[4], to comply with a request for the provision of advice, analysis or information for the department. DESNZ, with input from Ofgem, have asked NESO to provide recommendations based on their system and sectoral expertise on how to ensure the NIS Regulations capture our most critical operators in a changing energy landscape. DESNZ will consider these recommendations and evaluate whether amendments to NIS thresholds are appropriate and proportionate and will reconsult the sector.

Intermediate requirements

We acknowledge that the support for intermediate requirements (above baseline but below NIS) was mixed and that there was a strong consensus for any intermediate requirements to be considered once baseline requirements are implemented, and the NIS applicability review has been completed and implemented.

Some respondents disagreed with the need for intermediate requirements, due to sufficient coverage of existing frameworks, the potential for regulatory complexity and burden, the lack of evidence and the dynamic nature of the energy sector. Responses indicated some common themes on the risks intermediate requirements should look to address and who they should target (if pursued).

Based on the responses and the mixed support for intermediate requirements, we intend to focus on implementing baseline requirements and reviewing NIS applicability. Once these changes are established, government will review the effectiveness of NIS amendments and baseline requirements, and we will consult NESO, NCSC and industry to re-evaluate the need for intermediate requirements. We will use the feedback from this consultation to shape our evidence review and to guide further consultation work to gather views on any future proposals. Considering our strategy commitment to ensure that cyber resilience is raised across the whole DGE system by introducing a baseline level of cyber resilience to all involved parts, by the end of 2030, we anticipate that any consideration of intermediate requirements will be post 2030.

[4] Energy Act 2023

2.2.2 NIS Applicability Requirements

We sought views on whether current NIS thresholds for DGE essential services effectively captured operators, and how they should be amended. We also asked for views on what additional services should be brought into scope of the NIS thresholds, including appropriate thresholds and industry's rationale.

2.2.2.1 Question analysis

Q6. Do you consider that the current thresholds for the DGE essential services already captured by the NIS Regulations (see Table 7) effectively capture operators of essential services? If not, which thresholds should change, why, and in what direction?

Table 7: DGE essential services and thresholds under the NIS Regulations[5]

Essential Service	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 load control will be brought into scope of the NIS Regulations through 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.*

Table 8 below outlines respondents' answers to Question 6.

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

Table 8: Question 6 response breakdown

Response	Nr of responses	% of responses
Yes, the current thresholds effectively capture operators of essential services	7	~14%
No, the current thresholds do not capture operators of essential services	17	~35%
Unsure	21	~43%
No response	4	~8%
Totals	**49**	**100%**

Overall, respondents were unsure whether the current thresholds for the DGE essential services already captured by the NIS Regulations effectively capture operators of essential services. Some of these respondents felt that NESO, DESNZ and Ofgem were best placed to determine whether the thresholds were set appropriately.

Some respondents who were unsure still suggested changes to the thresholds, so the following numbers do not exactly align with the above percentages.

The main categories of thresholds respondents suggested should change were the electricity generation threshold (19 respondents); the supply/customer number threshold (15 respondents), the load control/battery energy storage system threshold (5 respondents) and the offshore and onshore transmission thresholds (4 respondents).

The primary reasons given for these changes were:

- That thresholds should be more risk or impact driven, rather than using purely a supply or generation approach (21 respondents);
- That the energy sector is interconnected and relies on digital systems and therefore the thresholds need to be updated to reflect categories of operator which are systematically significant without meeting current thresholds (20 respondents);
- That the energy sector has undergone significant changes and become much more of a distributed system, and therefore the current thresholds do not reflect how risks can arise with smaller operators (19 respondents); and
- To account for the risk posed by aggregated or coordinated services (16 respondents).

A smaller group of respondents felt that the current thresholds remain broadly appropriate. Their view was that baseline requirements would address cyber security gaps and warned against placing unnecessary regulatory burden on smaller operators who do not pose a comparable level of system risk. Of the 7 organisations that felt the current thresholds were sufficient, all were Ofgem licensees and 4 were organisations already within the scope of the NIS Regulations.

Q7. 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).

Table 9 below outlines respondents' answers to Question 7.

Table 9: Question 7 response breakdown

Response	Nr of responses	% of responses
Yes, there are additional DGE services that should be defined as essential services under the NIS Regulations	19	~38%
No, there are not additional essential services	14	~29%
Unsure	2	~4%
No response	14	~29%
Totals	**49**	**100%**

Responses were mixed on suggesting additional DGE services to be defined as essential services under the NIS Regulations. Service providers and non-licensed respondents were broadly more supportive of adding additional services, whereas Ofgem licensees were more mixed in whether they suggested additional services.

14 respondents did not support adding further services at this stage because they thought the current essential services definitions were sufficient and that the CSRB would address risk gaps.

However, 19 respondents did suggest additional service categories. These were:

- Flexibility services, aggregators and orchestration platforms (centralised software systems that coordinate, monitor and automate distributed energy resources such as EV chargers, solar arrays and batteries) (8 respondents)
- Digital and data platforms (6 respondents)
- System stability service providers (6 respondents)
- Remote monitoring and management providers (6 respondents)
- Electric vehicle charging infrastructure (3 respondents)
- Storage and battery energy storage systems (3 respondents)

It should be noted that some storage and battery energy storage systems, flexibility services and aggregators may fall within the definition of a large load controller (LLC), which refers to an organisation that remotely controls electrical load across energy smart appliances via digital

signals. These will be in scope of the NIS regulations where aggregate controllable load reaches or exceeds 300MW, as proposed in the CSRB.

It should also be noted that some of the service categories suggested by respondents may be affected by wider cyber regulatory reforms being introduced through the CSRB, including provisions relating to Relevant Digital Service Providers (RDSPs) and Relevant Managed Service Providers (RMSPs). The applicability of these provisions will be considered separately as part of the implementation of the CSRB.

Other proposed services, which received less consensus across responses, were shared resource providers, generators and absorbers of reactive power, customer facing and market services, smart metering communications, operations and maintenance, small modular reactors, offshore-onshore transmission, load control, heat networks, payment meters, smart appliance manufacturers, onshore transmission and arm's length bodies.

Q8. 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.

28 (57%) respondents did not answer this question. The majority who did answer suggested approaches for setting thresholds rather than quantitative benchmarks. Many expressed preferences for approaches based on system impact and functional criticality rather than organisational size alone.

The categories of approaches for setting thresholds suggested by respondents were:

- Risk, dependency or impact-based thresholds, which reflect real operational impact (14 respondents)
- Thresholds based on cumulative or aggregated impact (9 respondents)
- A dual or multi threshold model, combining quantitative indicators with qualitative assessment of systemic relevance (5 respondents)
- Alignment with existing benchmarks (4 respondents), including aligning new services with current NIS thresholds
- For specific services, having no thresholds, instead having all of that type of service in scope (2 respondents)

6 respondents suggested specific, quantitative thresholds. These included:

- Organisations with operational access to the NIS-regulated systems of more than five DGE operators, or remote management connections to more than 50 DGE sites (for remote monitoring and management providers)
- Organisations with aggregated controllable capacity above 100MW, or operational connections to more than 500 individually controllable sites

- More than 10,000 grid-interactive charge points with bidirectional capability, or aggregated controllable capacity above 50MW (for EV charging network operators)
- 50 MW (for load control)
- 200 MW or 500 MW (for generation)

2.2.2.2 Government Response

We welcome the broad range of views shared on our proposals to review the scope and thresholds of the NIS regulations for the DGE sector. A significant proportion of respondents agreed with the suggestion that the current thresholds for DGE do not effectively capture operators of essential services, with some also suggesting additional DGE services to be defined as essential services under the NIS regulations. We appreciate the concerns raised by many that thresholds based solely on customer numbers or generation (measured in GW capacity) are no longer appropriate given the modern, distributed and digitally integrated energy landscape. Some respondents believed that a more holistic, risk-based approach should be taken to capture smaller organisations which, if impacted by a cyber-attack, could cause widespread system failure.

The broad range of measures contained in the CSRB should make considerable improvements to cyber resilience across essential services, including DGE. In the consultation document, we noted that regulatory requirements applying to the supply chain and large load controllers were out of scope of this consultation, as the cyber requirements for these organisations are being considered separately through the CSRB.

The NIS Regulations are designed to capture the most critical organisations and boost their level of cyber security across network and information systems. We acknowledge some respondents' views that new measures proposed in the CSRB, combined with our proposal of baseline requirements, would be sufficient cyber regulation, and would make an impact without the need to further broaden the scope of the NIS Regulations. Whilst the CSRB will provide the powers required to ensure the scope of NIS keeps pace with the evolving energy system, the scope of the review itself is still for DESNZ to lead and implement. When reviewing the thresholds, we will focus on proposing amendments that are based on risk and impact evidence, in order to address cyber resilience gaps across critical operators while also ensuring NIS regulation remains targeted. As part of this, we will also consider any wider regulatory changes and potential impacts on the DGE sector, including any changes resulting from dynamic alignment with European Union laws via the Electricity Agreement and powers in the European Partnership Bill.

An anonymised consolidation of the responses relevant to the NIS thresholds has been shared with NESO to support their review. Ofgem and DESNZ have commissioned from NESO a review of the categories of essential services and thresholds under the NIS Regulations for DGE. Government will consider the recommendations made by NESO, alongside risk appetite, regulatory burden and current and future cyber threat to determine whether the definitions and thresholds of essential services need to be updated.

If DESNZ, working with partners and based on NESO analysis, concludes that these updates are needed, proposed revised definitions and thresholds will be subject to further consultation with industry and relevant stakeholders.

2.2.3 Baseline Requirements

We sought views on introducing baseline cyber resilience requirements for all Ofgem licensees, including the suitability of Cyber Essentials (CE/CE+) as the foundation. We also invited feedback on whether CE Controls are sufficient or should be expanded, alternative frameworks and perspectives on costs, barriers, certification experience and a wider use of cyber standards.

2.2.3.1 Question analysis

Q9. What are your views on the proposed principles for baseline requirements? Please explain the reasoning for your response.

Table 10 below outlines respondents' position on Question 9.

Table 10: Question 9 response breakdown

Response	Nr of responses	% of responses
Agree with principles for baseline requirements with no changes	20	~41%
Broadly agree with principles for baseline requirements and make extra recommendations	23	~47%
Disagree with principles for baseline requirements	3	~6%
No response	3	~6%
Totals	**49**	**100%**

Respondents were asked to provide their view on the proposed principles for baseline requirements. Those principles are set out below for reference:

Baseline requirements should:

- provide protection against the most common cyber attacks
- be low burden for organisations to implement
- be a starting point, not a final target. Licensees should build on these requirements based on their business-specific context and individual risk assessment
- be independently assured to verify their effectiveness
- be shaped via consultation with NCSC
- be delivered through licences and be applicable to all Ofgem licensees

Overall respondents were supportive. 88% of respondents (43) either agreed with the proposed principles unchanged or broadly supported them subject to additional considerations.

Among those who proposed additional considerations, most focused on advocating for additional controls, which are addressed in Question 11. Therefore, few changes were suggested to the principles themselves. The main themes arising regarding the principles were:

- To ensure proportionality, avoiding one size fits all solutions
- To ensure continuous improvement

Q10. 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.

Table 11 below outlines respondents' position on Question 10.

Table 11 Question 10 response breakdown

Response	Nr of responses	% of responses
Agree with CE/CE+ as a starting point	20	~41%
Agree with CE/CE+ as a starting point but raise additional considerations	17	~35%
Disagree with CE/CE+ as a starting point	8	~16%
No response	4	~8%
Totals	**49**	**100%**

Most respondents (76%) were in favour of using the Cyber Essentials scheme (CE/CE+) as the basis for shaping a baseline requirement, either without changes (41%) or subject to additional considerations (35%). Of the 76% (37), 25 were Ofgem licensees, 15 of which were OES. The remaining 12 were non-licensees, primarily cyber security providers or consultancies.

Reasons for support included that the scheme is:

- Well established, cost-effective, accessible and a widely understood framework
- Aligns with basic cyber hygiene practices
- Will help raise the baseline security standard across the sector

Of the 17 respondents who supported the use of the Cyber Essentials scheme subject to additional considerations, the most cited considerations included:

- Existing controls are IT focused and not adequate for Operational Technology (OT)
- The need to avoid additional regulatory burden or duplication for those subject to existing requirements

- A preference for not introducing a bespoke scheme

Additional recommendations included:

- Preferred use of CE+ over CE to provide a higher level of independent verification and ensure consistent assurance
- Position Cyber Essentials as a foundational baseline only

8 respondents disagreed with the use of the Cyber Essentials scheme (CE / CE+). The primary reasons given were:

- The existing controls are not adequate for Operational Technology (OT)
- Suitability for larger organisations due to the complexity of their estates and the difficulty in implementing prescriptive controls
- Alignment with internationals standards and perceptions that it represents a low bar compared to existing standards and frameworks.

In addition to views on a Cyber Essentials scheme forming the basis for a baseline requirement, respondents were asked whether the existing five controls were adequate or whether to go beyond the controls by developing a bespoke scheme. 28 respondents supported going beyond the existing controls. Of these, 25 favoured using CE/CE+ as the foundation from which to build upon and enhance. The remaining 3 respondents called for the use of existing frameworks or standards and opposed the development of a bespoke scheme. The main concerns were related to cost, creating confusion across the sector and being resource intensive to design and implement.

Q11. 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?

Figure 1 below outlines respondents' position on Question 11.

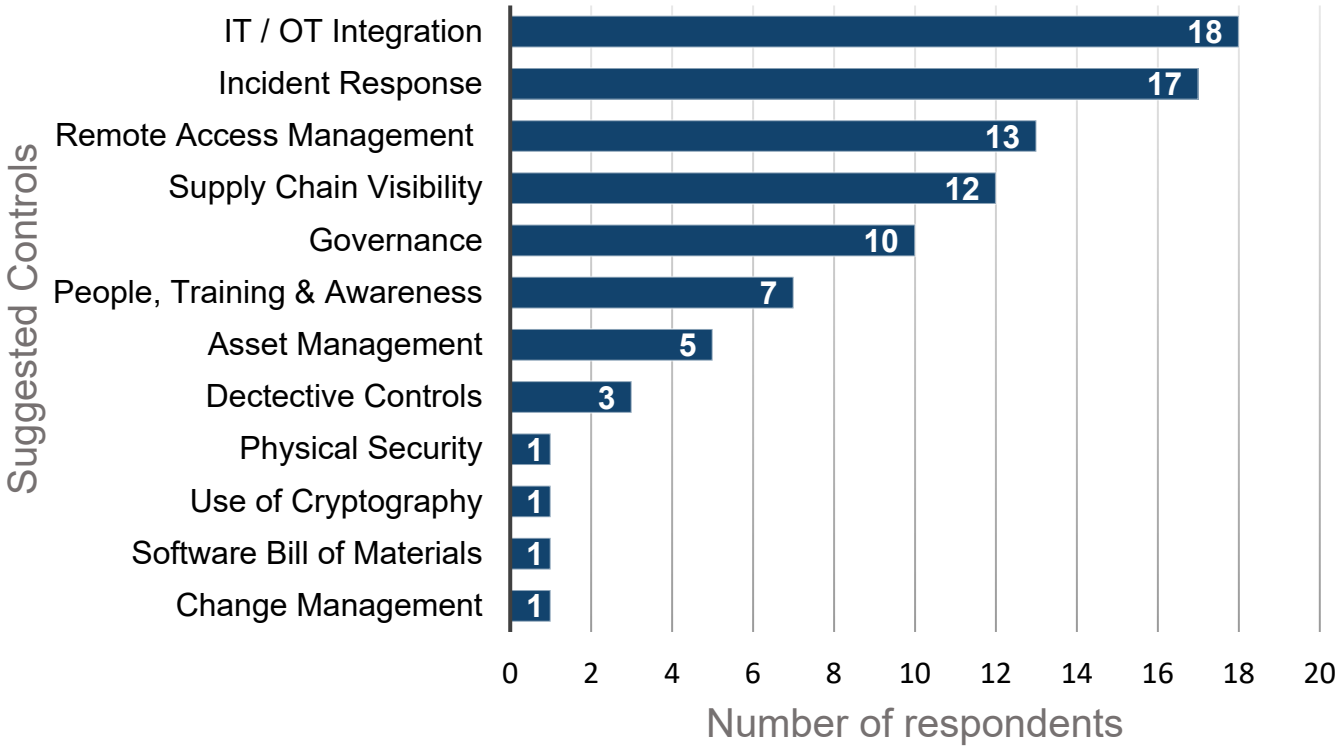

Figure 1: Question 11 response breakdown*

**N.B. The figures represent multiple controls suggested by individual respondents.*

Respondents provided a range of suggestions for additional controls to inform the development of a baseline requirement. While views varied, several themes emerged consistently across responses, indicating areas of priority for strengthening cyber resilience.

The key controls emerging were:

- IT / OT Integration / Network Segmentation;
- Incident Response/ Exercising;
- Remote Access Management;
- Supply Chain Visibility;
- Governance;
- People Training & Awareness

In addition to controls, respondents also advocated for:

- The provision of guidance; sector specific guidance on implementing baseline requirements and for operational technology (OT).
- Co-ordination across government, such as the sharing of threat intelligence.
- Greater cross-sector collaboration.

Q12. 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.

Table 12 and Figure 2 below outline respondents' answers to Question 12.

Table 12: Question 12 response breakdown

Response	Nr of responses	% of responses
Yes, consider alternatives to CE/CE+	25	~51%
No alternatives to CE/CE+ proposed	14	~29%
No response	10	~20%
Totals	**49**	**100%**

As can be seen from Table 12, more than half of respondents (25) suggested alternatives to the Cyber Essentials scheme for baseline requirements. Of these, 19 also supported the use of CE/CE+ as a baseline requirement, which implied that their suggestions were intended to complement rather than replace the proposal.

A further 14 respondents did not propose alternative suggestions. 12 of these were supportive, or broadly supportive subject to additional considerations of using CE/CE+.

It should be noted that some respondents interpreted the 'Cyber Essentials scheme' to be CE rather than CE+. In these cases, respondents often recommended CE+ as an alternative standard for baseline requirements, as they considered CE to be our proposal and considered this to be less comprehensive than CE+. CE+ has been excluded from Figure 2 below, to avoid its misinterpretation as an alternative framework to our proposed basis for baseline requirements.

The most recommended standards, certifications and frameworks proposed for consideration were:

- Cyber Assessment Framework (CAF)
- IEC 62443
- ISO 27001
- NIST SP 800 – XX (different variants were suggested)
- NIST CSF

Figure 2 outlines the response breakdown to question 12, listing additional' proposed frameworks and standards for government consideration.

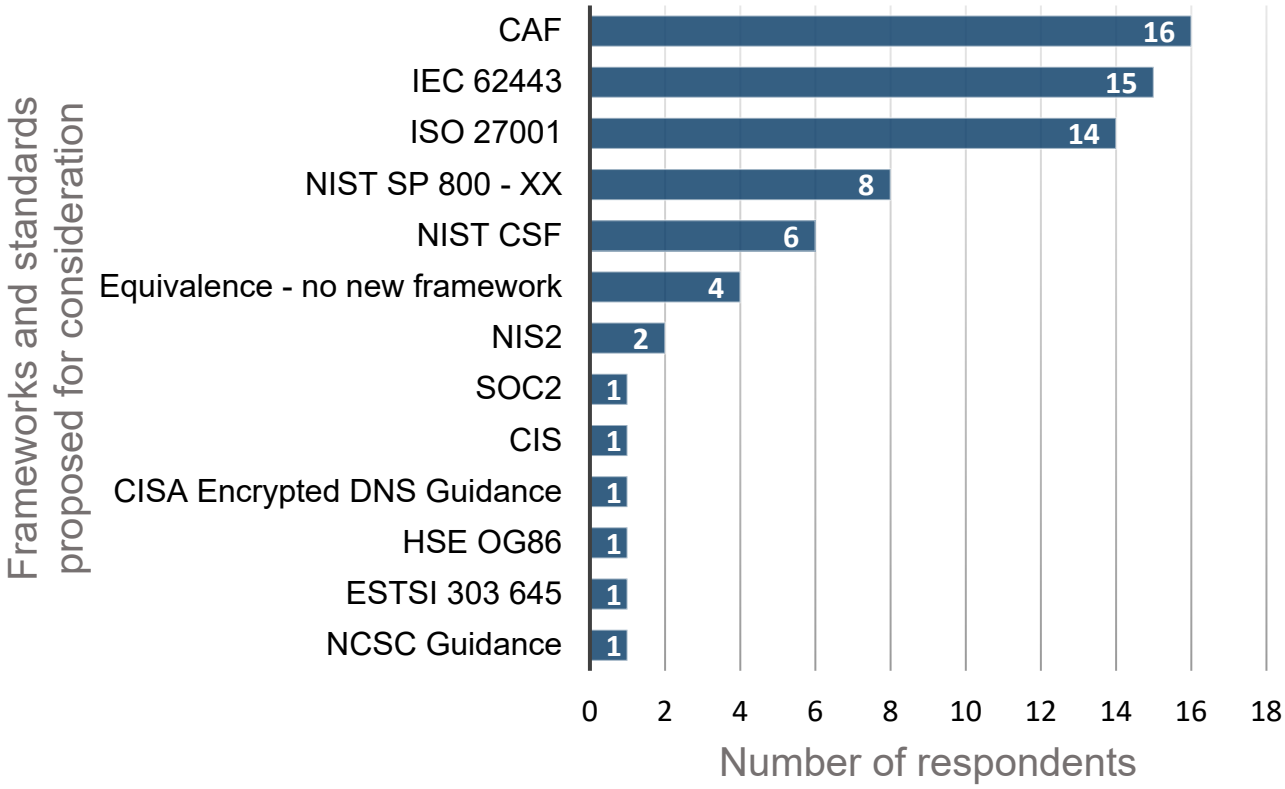

Figure 2: Question 12 response breakdown

**N.B. The figures represent multiple frameworks and standards suggested by individual respondents.*

The results show that there was no clear consensus on an alternative scheme/ framework/ standard. Respondents did not recommend any one single framework as a comprehensive solution.

Q13. 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)?

Table 13 below outlines respondents' position on Question 13.

Table 13: Question 13 response breakdown

Response	Nr of responses	% of responses
Unable to quantify CE/CE+ certification costs	5	~10%
Costs cited as <£10,000 or low/ modest	4	~8%
Costs cited between £10,000 and £100,000	1	~2%
Costs cited as > £100,000	3	~6%
No response	15	~31%
Not applicable	21	~43%
Totals	**49**	**100%**

As can be seen in Table 13, when asked about CE/CE+ certification costs, the question was either not applicable or not answered by 36 respondents. These respondents were either licensees that have never held CE/ CE+ certifications, or individuals/ organisations that had no experience of working with Ofgem licensees holding a CE/CE+ certification.

The cost position across the remaining 13 responses was mixed. Lower costs were generally associated with smaller/ lower complexity organisations that had a good starting point of maturity, while higher costs were driven by multi-entity structures, scope complexity, legacy and OT-heavy environments, and a low starting maturity. The prescriptiveness of the CE controls and the inability to allow for compensating controls were also cited as common issues driving costs up.

Q14 & Q15: CE/CE+ barriers

Q14. 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.

Q15. 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?

Questions 14 and 15 are grouped together due to them both relating to barriers faced by organisations in their journey to obtain CE/CE+ certification. Question 14 asked for the perspectives of those that hold (or have held) those certifications, when Question 15 was aimed at those that do not. Similar themes were cited across both groups.

Table 14: Question 14 response breakdown

Response	Nr of responses	% of responses
Ofgem licensees that hold or have held CE/CE+ certification and faced barriers	6	~20%
Ofgem licensees that hold or have held CE/CE+ certification and did not face barriers	7	~23%
Unsure	2	~7%
No response	11	~37%
Not applicable	4	~13%
Totals	**30***	**100%**

*30 is the total number of responses received from Ofgem licensees

Table 14 shows the number of licensees that hold or have held CE/CE+ certifications that faced barriers to achieving this. Out of the 6 licensees that reported facing barriers, 5 were large organisations (>499 employees) and one did not provide their organisation's size. Out of the 7 licensees that reported facing no barriers, 5 had less than 250 employees and 2 had more than 499 employees.

The barriers cited were largely related to business size and OT presence leading to scope complexity, and to the prescriptiveness of CE/CE+ controls without the ability to use compensating controls to demonstrate compliance.

Similar barriers were also the dominant themes in Question 15 which was targeted to organisations who do not hold CE/CE+ certifications. Some additional barriers that were listed by this group related to duplication with existing cyber requirements/ certifications and resource/ time requirements. respondents listed the prioritisation of international standards and challenges in getting re-certification support.

2.2.3.2 Government Response

Government welcomes the overall support for the proposed principles and for using the Cyber Essentials scheme as a basis for shaping baseline requirements for all Ofgem licensees. We welcome the addition of continuous improvement to our principles and intend to reflect this feedback in the further development of the baseline resilience requirements proposals.

We also acknowledge that some respondents encouraged us to ensure that baseline requirements are proportionate. Ofgem and DESNZ intend to shape baseline requirements to be a proportionate starting point for the wide audience they are intended for – which is all Ofgem licensees. However, it is important to note that government expects licensees to apply the proportionality principle to their individual risk context, and use baseline requirements as the foundation on which to build on and go beyond based on their individual circumstances and risk assessment, rather than relying solely on the baseline requirements themselves. We will

also ensure proportionality is appropriately considered as part of the NIS applicability review and in the development of any future intermediate requirements (should this proceed).

We acknowledge the broad support for building on the Cyber Essentials scheme rather than developing a new scheme. Respondents generally favoured using CE+ rather than CE as a foundational baseline due to the independent assurance, which was seen as beneficial. They were also in favour of supplementing CE+ with additional controls and guidance to address sector specific risks.

We acknowledge the concerns respondents raised about the limitations of CE/CE+ for the energy sector, in relation to the exclusion of Operational Technology (OT) environments and the scheme's suitability for larger or more complex organisations, particularly due to the prescriptiveness of the Cyber Essential scheme's controls and the need to demonstrate compliance through strict adherence to the controls. There were also broader concerns related to alignment across existing frameworks and regulatory burden for those subject to existing cyber resilience requirements. Whilst a range of alternative or complementary approaches, standards, certifications and frameworks were proposed in addition to the Cyber Essentials scheme, views were mixed with no clear consensus on a single framework. We recognise these concerns and intend to draw on existing frameworks with a view to ensuring alignment and delivering an approach that avoids unnecessary burden.

Having carefully considered the feedback we received, we have shaped our response on five key areas:

Use of Cyber Essentials scheme as a starting point for baseline requirements

Given the broad support expressed through this consultation, we intend to use the Cyber Essentials Scheme as the foundation to shape baseline cyber resilience requirements for all Ofgem licensees. As highlighted in the consultation, we want to emphasise that this is a starting point on which organisations can build their cyber resilience rather than a complete solution. Organisations are expected to assess their individual risk context and – if appropriate - go beyond the baseline requirements by implementing additional cyber resilience measures.

Choice between CE and CE+

We intend to use CE+, reflecting the broad agreement with our principle for baseline requirements to be independently assured, as well as the preference expressed in the consultation for CE+ over CE and for the use of an established scheme. We acknowledge that CE+ offers the added benefit of a higher level of independent assurance than basic CE, which will provide a more consistent baseline across the sector.

Going beyond the controls of CE+

We recognise that CE+ has limitations for the energy sector, such as in relation to the exclusion of Operational Technology (OT), and the lack of controls related to governance, incident response, risk management, and supply chain management (as it is more technology focused). We therefore welcome the call to go beyond the CE+ control families, and we will

consider these areas as part of our future policy development. Ofgem will further consult with the sector as part of the detailed design phase and work closely with the NCSC who will provide the technical expertise and advice needed to develop the appropriate additional controls and guidance. Our intention, subject to further planning alongside NCSC, is to further consult on baseline requirements and initial implementation proposals in 2027.

Supporting complex / OT heavy organisations to attain CE+

We acknowledge the challenges that larger / more complex organisations face in attaining CE+ certification. To address this, Ofgem and DESNZ will work closely with NCSC to explore the potential of using [6]. Cyber Essentials Pathways provides tailored support through specialist assessors and the ability to demonstrate compliance with the Cyber Essentials scheme controls more flexibly. It is intended to help organisations achieve certification where the standard approach may be too prescriptive within a more complex environment. We will consider its suitability and any alternative approaches as this work progresses.

Minimising regulatory burden and duplication

We are committed to ensuring that baseline requirements are implemented in a way that minimises regulatory burden and avoids duplication where existing requirements already apply. We understand that a proportion of licensees are OES under NIS, subject to the Smart Energy Code (SEC) (energy and electricity suppliers), or are Load Controllers who will soon be subject to cyber resilience requirements through licences. We are also aware that the Electricity Agreement and subsequent powers in the EU Partnership Bill have the potential to impact UK cyber regulation for organisations involved in cross-border electricity flows, which may introduce additional cyber requirements on a subset of Ofgem licensees.

We do acknowledge that cyber resilience requirements already exist for a sub-set of Ofgem licensees (OES, SEC, Load Controllers). However, they do not cover the full extent of licensees' network and information systems, due to defined scope limitations (e.g. cyber security requirements may apply to subsets of systems, leaving parts of the network and information systems estates of licensees unprotected). Baseline requirements are intended to have a broader scope to help defend against the most common attacks.

Taking the above into consideration, we agree on the need to minimise duplication and regulatory burden. To achieve this, our intention is that - where possible - baseline requirements should only apply to systems not covered by existing cyber resilience requirements.

We will also work to further understand the impact of the Electricity Agreement and subsequent powers in the European Partnership Bill on our proposals. This work may introduce further cyber resilience requirements on a subset of Ofgem licensees. We will develop policy options on how baseline requirements can be implemented while minimising duplication and burden, considering all applicable existing cyber requirements.

[6] NCSC Cyber Essentials Pathways

Ofgem and DESNZ will use the consultation responses to further shape the development of more detailed proposals for baseline requirements. We intend to consult further on the details, design and implementation of baseline requirements before we finalise the approach.

3 Next steps

The feedback received as part of this consultation process is being considered carefully as we further develop this policy. We will be engaging with the sector on further policy proposals in a range of areas, including plans for Ofgem to consult within 2027 on proposed baseline requirements and their initial implementation proposals, and DESNZ to consult within 2027 (subject to CSRB Royal Assent) on proposals for revised NIS thresholds and essential services. Further engagements will follow to finalise policies, including consulting with the sector on intermediate requirements (if it is decided there is merit in pursuing these) after the NIS applicability review has concluded and baseline requirements have been implemented (beyond 2030). DESNZ and Ofgem will also continue to work with key partners including NESO, NCSC and DCMS who will provide expert advice and guidance.

As cyber threats evolve and the energy system changes in support of the government's Clean Power Mission, the cyber regulatory landscape must keep pace. The recently published Energy Sector Cyber Security Strategy[1] outlines the government's ambitions to ensure the energy sector is resilient against cyber-attacks in the current landscape and makes clear the expectations on industry to strengthen their cyber security postures.

In the Energy Sector Cyber Security Strategy, we made the following public commitments:

- To assess the NIS regulatory thresholds, including whether new critical sub-sectors need to be captured, by the end of 2027
- To shape proposals for introducing baseline cyber resilience requirements for all Ofgem licensees, by the end of 2027
- To ensure that cyber resilience is raised across the whole DGE system by introducing a baseline level of cyber resilience to all involved parts, by the end of 2030

This government response has set out our position after considering stakeholder feedback and our plans towards achieving these commitments.

We recognise that expanding regulation to broader settings creates a risk of additional burden, particularly considering that regulatory reform in DGE is only one element of change within a broader landscape of activity on cyber security. DESNZ and Ofgem are therefore working to ensure that requirements for the DGE sector are streamlined and effective.

We will be actively monitoring any cyber regulation implications of the Electricity Agreement and powers in European Partnership Bill to ensure they are factored into our policy development. We are also working in partnership with DCMS during the CSRB's progress through parliament to understand the consequences on the DGE sector. The CSRB is expected to receive royal assent in early 2027.

If – following NESO's advice and considering the responses submitted to this consultation – government concludes that there is a need to amend the DGE NIS-defined essential services

and thresholds, we aim to consult with the sector on these changes within 2027 and leverage CSRB powers to implement them.

4 Glossary

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
DCMS	The Department for Culture, Media and Sport
DESNZ	The Department for Energy Security and Net Zero
DGE	Downstream Gas and Electricity
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: Whole energy cyber resilience requirements: reshaping cyber regulation in downstream gas and electricity - GOV.UK

Any enquiries regarding this publication should be sent to us at: Cyber.Policy@energysecurity.gov.uk and 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.