Final stage impact assessment

Title:	Load Control Licensing
Department or agency:	Department for Energy Security and Net Zero
Contact for enquiries:	SSES.Licensing@energysecurity.gov.uk
Date:	10 December 2025

1. Summary of proposal

The Government intends to create a new licence for organisations involved in electric load control services in order to protect consumers and the electricity system from unacceptable risks associated with the control of energy smart appliances for the purpose of consumer led flexibility (CLF). Ofgem, as with other electricity system licences, will be the regulating authority for the new licence.

2. Strategic case for proposed regulation

Moving to a smarter and more flexible energy system is crucial for delivering the government's Clean Energy Superpower mission. Great Britain (GB) increasingly needs sources of low carbon flexibility to facilitate a move away from a carbon-intensive system, in which unabated gas plays a major role in providing security of supply and electricity is generated by a small number of large power stations.[1] GB electricity demand is expected to increase significantly, due to the electrification of heat and transport sectors,[2] and supply of that will be through large quantities of intermittent renewables. System flexibility will be vital for shifting demand away from peak periods and utilising clean electricity when it is abundant, thereby ensuring the most cost-efficient system.

Low carbon flexibility can be provided by a range of sources, such as batteries, long duration electricity storage and consumer-led flexibility (CLF). CLF refers to actions taken by consumers to shift the time of their electricity use, typically to save money by accessing electricity at cheaper times of the day or to gain value from providing flexibility to others. CLF differs from energy efficiency and demand reduction, both of which involve reducing total

[1] The National Energy System Operator (NESO) estimates that in 2024 around 50% of all electricity was produced using carbon-based fuels. NESO, 'Britain's Electricity Explained: 2024 Review' (viewed on 8 December 2025)

[2] Currently, GB national demand is 330 TWh per annum. Depending on how we reach net zero, demand is expected to increase to between 450-500 TWh by 2035 and between 570-770 TWh by 2050. GOV.UK, 'Electricity networks strategic framework' (viewed on 8 December 2025)

demand rather than shifting demand to economically more optimal times, or to times when less stress is placed on the grid.

A central subcategory of CLF is "load control", where an organisation directly controls the electricity consumption of an Energy Smart Appliance (ESA)[3] in line with market conditions to generate savings and revenue for the ESA owner. In the electricity system, load control is carried out by Flexibility Service Providers (FSPs) and Load Controllers (LCs). They connect consumers and their appliances to electricity markets. FSPs are consumer facing organisations that contract with consumers to shift electricity consumption and remunerate them for it. LCs remotely control consumer appliances (through load control signals ultimately sent to the ESA) in line with their preferences and electricity market opportunities to earn revenues. It is also possible for organisations to operate in both roles.

The number of households and appliances controlled through FSPs and LCs as well as the corresponding CLF capacity provided to the grid is rising. In 2024, according to the National Energy Systems Operator (NESO), there was 1.6 GW of consumer-led flexibility utilised in GB (not including electric storage heater flexibility), with 0.2 GW coming from smart heat pumps and flexible district heating, 0.2 GW from EV smart charging, 0.3 GW from other smart appliances and 0.8 GW from non-domestic consumer-led flexibility.[4] With the further take-up of Energy Smart Appliances (ESAs) and a larger number of flexibility service offerings, there is considerable growth potential led by a broader base of consumers.[5] Based on NESO and DESNZ scenarios for 2030, we expect to enable 10-12GW of consumer-led flexibility capacity (excluding electric storage heaters) by 2030 to support clean power.

Increasing consumer engagement in CLF exposes the electricity system and consumers to cyber security and consumer protection risks.

- Cyber security: LCs will be able to remotely control significant amounts of electrical load through EV chargepoints, heat pumps etc. Without proper cyber security protections, an attack on a large number of devices, organisations, or supporting platforms could have serious consequences. An attacker that seizes control of many devices – or the systems used by organisations to control them – would be able to freely shift large volumes of demand up or down. If the amount of demand they control is large enough, they could cause damage to critical national infrastructure (CNI), with a consequent interruption of electricity supply to consumers that could potentially cause harm to life where consumers are critically dependent on that electricity supply. NESO estimates that an unplanned and sudden shift in 300MW of electrical load, via a cyber-attack, at times when the grid is under stress (for instance a calm, cloudy winter afternoon) could trigger blackouts. Potentially, attacks involving much smaller amounts of load could impact local infrastructure, e.g. causing the fuse at a local substation to 'trip'. Some organisations already control well above this level of electrical load, and, unlike traditional actors in the energy sector (such as unabated

[3] In the context of the load control licence only appliances which can shift significant loads are referred to as ESAs such as EV charge points, domestic batteries as well as electric heat appliances. GOV.UK, 'Smart Secure Electricity Systems Programme: Licensing Consultation, Proposals on load control licence regulations and licence conditions' (viewed on 9 December 2025)

[4] NESO, 'Future Energy Scenarios' (viewed on 8 December 2025)

[5] Ofgem's State of the market report shows that between January 2024 and January 2025 the number of households using time of use tariffs grew by 70% from approximately 400,000 to 660,000. Ofgem, 'State of the energy market report: retail' (viewed on 8 December 2025)

gas generators and DNOs), they are not currently subject to oversight or regulatory requirements to provide assurance that appropriate cyber security protections are in place.

Cyber-attacks on the energy sector are a real threat today. In the Cyber security breaches survey 2025 approximately 70% of medium and large businesses stated that they were subject to a cyber-attack in the last 12 months.[6] The energy sector is the main target of attackers.[7]

- Consumer protection: Poor consumer treatment leads to low levels of consumer trust which is essential to ensure mass uptake of CLF. With new companies entering a growing but unregulated CLF market, the risk of "bad actors" entering, who are unable or unwilling to uphold consumer protection standards, rises too. New types of flexibility services and products come with potential risks of mis-selling or contractual obligations that "lock in" consumers to using devices or services (like the early days of mobile phones when consumers faced barriers to switching mobile service operators). Further, there is a risk that consumers could purchase an expensive device and then find they receive poor quality service but are unable to change their service provider unless they replace the device.[8]

The potential damage to the UK were these risks to materialise is often larger than the value of the companies in scope. Hence, companies are not adequately incentivised to invest in consumer protection and cyber security resulting in potential **negative externalities**. Other **market failures**, such as **information asymmetry** or **market power** are also present in the domestic CLF market. These are discussed in detail in the evidence base section of this document.

Without government intervention these risks will not be mitigated and over time could translate into consumer detriment and real economic damage. The 2019 Cyber Security Incentives and Regulation Call for Evidence[9] found that 71% of respondents agreed that a lack of strong commercial rationale was a barrier for effective cyber risk management. The 2025 Cyber Security Breaches Survey found that there is a clear lack of commercial interest in some companies to effectively negotiate a cyber security budget against other competing organisational priorities. The National Cyber Security Centre (NCSC) has also emphasised the need for intervention in the flexibility markets to mitigate cyber risk and has highlighted cyber proliferation and cyber threats to CNI as a key risk in its latest annual review.[10]

In terms of consumer protection, the energy supply market is a useful case study. Here Ofgem has to intervene every year to protect consumers from mistreatment from suppliers.[11] Consumers who engage in CLF to the benefit of the whole system also need protection. In

[6] GOV.UK, 'Cyber security breaches survey 2025' (viewed on 8 December 2025)
[7] According to IBM's X-Force Threat Intelligence Index 2024 the UK energy sector is main target of cyber attackers in recent years. IBM, 'The UK energy sector faces an expanding OT threat landscape' (viewed on 8 December 2025)
[8] This was the case with the first generation of smart meters (SMETS1), which often lost their smart functionality when customers switched energy supplier due to not being interoperable between different energy suppliers.
[9] GOV.UK, 'Cyber security incentives & regulation review: government response to the call for evidence' (viewed on 8 December 2025)
[10] NCSC, 'NCSC Annual Review 2024' (viewed on 8 December 2025)
[11] Ofgem, 'Enforcement cases' (viewed on 8 December 2025)

the absence of this, consumers could lose trust in taking up these services risking the delivery of the Government's CLF ambition.

3. SMART objectives for intervention

By implementing the load control licensing regime the government wants to meet the following objectives:

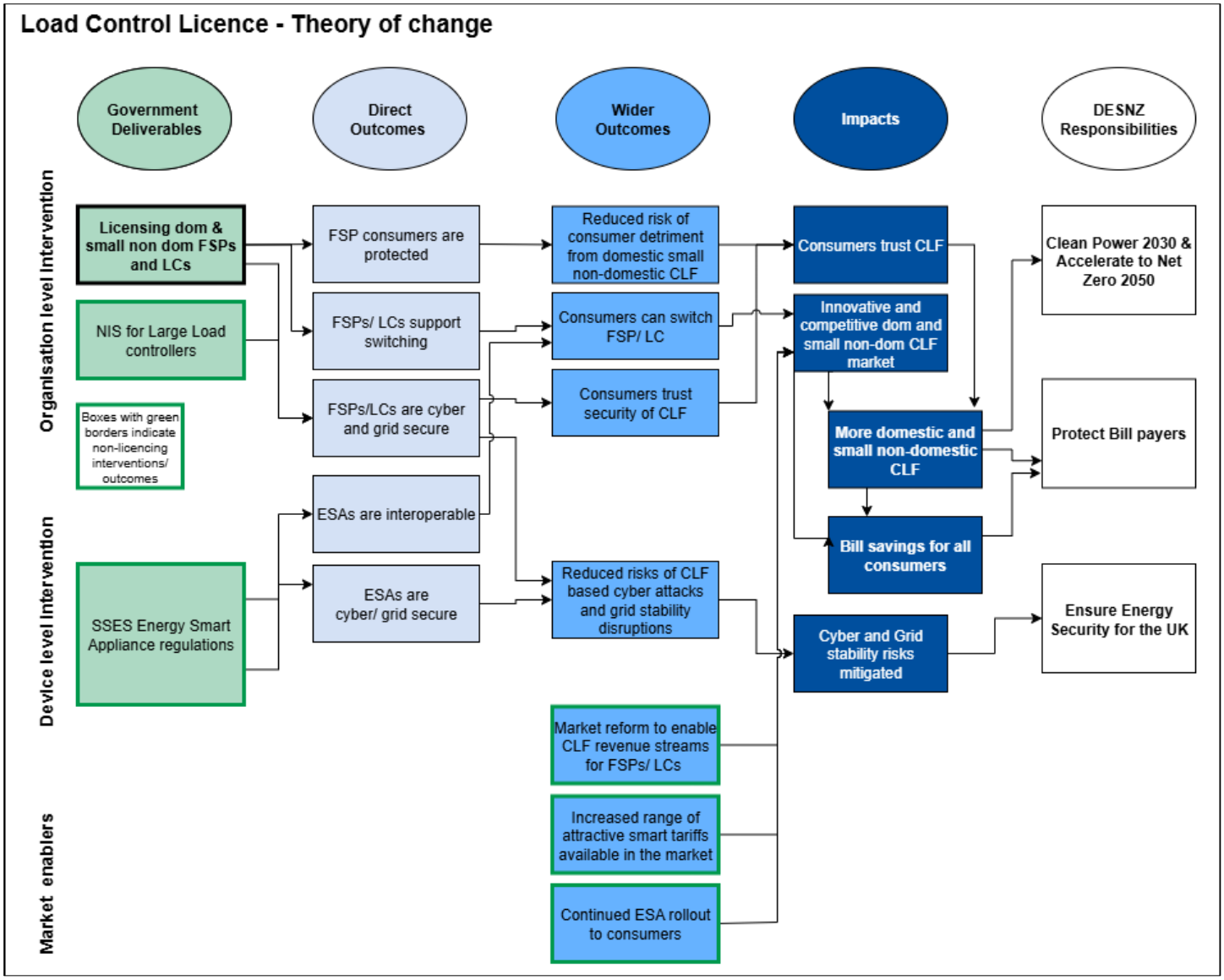
1) By 2028 enabling increased uptake of domestic and small non-domestic CLF through giving consumers confidence to engage with a smart energy system and create a level-playing field for participating companies.
2) By 2028 reducing the cyber security and grid stability risks to our electricity system resulting from the increased uptake of domestic and small non-domestic CLF.

The licensing regime will ensure that LCs are cyber- and grid-secure and that FSPs protect their consumers. This will contribute to consumer trust in CLF and mitigate CLF related risks to the electricity system. Alongside other enabling policies this will lead to higher consumer engagement with CLF to provide low-cost and zero-carbon flexibility to the electricity system. This directly supports the HMG objectives of making the UK a clean energy superpower.

4. Description of proposed intervention and explanation of the logical change process whereby this achieves SMART objectives

The government is planning to make load control a licensable activity under the Electricity Act 1989 and to create a new load control licence. The load control licence will stipulate requirements for FSPs to ensure they treat consumers fairly and for LCs to mitigate cyber and grid stability risks. The new licence will be enforced by Ofgem, who can take enforcement action against licensees failing to comply, thus ensuring that LCs are cyber and grid- secure and that FSPs protect their consumers. The logic model in Figure 1 shows how the licensing regime will contribute to increase CLF engagement and to meeting government objectives.

Figure 1: Load Control Licence - Logic Map



5. Summary of long-list and alternatives

The government considered the following long list of options to deliver the objectives:

- Option I: Do Nothing - Voluntary, industry led standards
  In a "Do Nothing" scenario FSPs and LCs would manage their consumer relations and cyber security according to their requirements. They may choose to accede to voluntary, industry led standards where these exist.

- Option II: Load control licence
  Government would create a new licence for organisations involved in load control services in order to protect consumers and the electricity system from unacceptable risks associated with the control of ESAs for CLF. To create this licence, Government will need to pass secondary legislation and draft licence conditions. Ofgem, as with other electricity system licences, will be the regulating authority for the new licence. Consumer protection and cyber security measures could be tiered leading to the following sub options.
    - Option IIa) Tiered consumer protection and cyber security

To soften the administrative burden on small and medium sized businesses, the consumer protection and cyber security requirements would be tiered. FSPs with fewer consumers below a certain threshold would be subject to softer requirements. For LCs a basic and an enhanced tier of requirements would be introduced depending on the level of load they control.

  - Option IIb) Tiered cyber security only
    To manage the administrative burden on smaller LCs and to scale cyber security protections in line with risk, a basic and an enhanced tier of requirements would be introduced. One set of consumer protection requirements for all FSPs.
  - Option IIc) Untiered licence
    All licensees would follow the same consumer protection and cyber security requirements.

- Option III: Load control licence + a new load control industry code
  In addition to the load control licence, a new industry code could be established between relevant industry parties (e.g., FSPs, Load controllers, suppliers, grid operators) administered with a new code manager licensed by Ofgem. This code could cover a variety of business-to-business arrangements to support domestic CLF. For example, agreed industry best practices on consumer communication around CLF, and arrangements on how a FSP and supplier interact when they are both supplying services to the same property.

All long list options were assessed according to four critical success factors: Strategic fit, Value for money, Affordability and Achievability. Voluntary standards leave an excessive risk of consumer harm or grid disruption as Ofgem would have no way of addressing organisations that drop below minimum expected standards. Hence, Option I was excluded due its poor strategic fit as the stated objectives of the licence are supporting consumer confidence and mitigating cyber security and grid risks. Introducing a new industry code (Option III) would risk creating excessive administrative burdens and stifling innovation in a nascent market and would be very complex and time consuming to implement for government. Hence, Option III was excluded due to weak strategic fit and poor achievability.

SaMB assessment

The preferred option is a load control licence. Government estimates that approximately 17 out of 45 companies in scope of the new load control licence are small or micro sized businesses. Introduction will always create administrative costs for licensees. As set out in the evidence base, small companies may face higher costs than large companies. Although, we are seeking to validate this finding through this consultation. To mitigate this impact different tiering options for the load control licence were tested. As set out in more detail in Table 21 tiering of consumer protection requirements was deemed not suitable to the core objective of the licence, whilst tiering of cyber security requirements has become the government's preferred option. Part of the rationale for deeming tiering of consumer protection requirements not suitable was due to decisions taken in our 2025 government response to phase consumer protection requirements. The small sample size of cost estimates received during the 2024 consultation are therefore reflective of a wider number of consumer protection requirements than are being proposed to be taken forward in this consultation (see 4.2.2 Costs to Business section for more details).

6. Description of shortlisted policy options carried forward

Following the long list appraisal, government considered the following short list of options.

- Option 1: Do Nothing - Voluntary, industry led standards
  In a Do Nothing scenario FSPs and LCs would manage their consumer relations and cyber security according to their requirements. They may choose to accede to voluntary, industry led standard where these exist.
  This option serves as counterfactual in the short list appraisal.

- Option 2: Load control licence with cyber security tiering (preferred option)
  Government would create a new licence for organisations involved in load control services in order to protect consumers and the electricity system from unacceptable risks associated with the control of ESAs for CLF. Ofgem, as with other electricity system licences, will be the regulating authority for the new licence. To manage the administrative burden on smaller LCs and to scale cyber security protections in line with risk, a basic and an enhanced tier of requirements would be introduced. One set of consumer protection requirements would apply to all FSPs.

- Option 3: Untiered Load controlled licence
  As in option 2 government would create a new licence for organisations involved in load control services. All licensees would follow the same consumer protection and cyber security requirements.

7. Regulatory scorecard for preferred option

Part A: Overall and stakeholder impacts

(1) Overall impacts on total welfare		**Directional rating** **Note: Below are examples only**
Description of overall expected impact	The load control licence will ensure crucial customer and cyber security protection in the load control market. The resulting support of consumer confidence will contribute to a stronger take up in CLF which should translate into lower electricity systems costs. Cyber security protections will contribute to the prevention of grid disruption and the associated economic damage. However, compliance with the load control licence creates new costs for FSPs and LCs, especially those not following requirements already.	**Positive** **Based on all impacts (incl. non-monetised)**
Monetised impacts	Benefits have not been monetised. The present value costs of the preferred option are £54m - £121m (2025 prices).	**Negative** **Based on likely £NPSV**

	Directional rating is only based on costs.	
Non-monetised impacts	Benefit: Increase of consumer confidence because of customer protection requirements to support CLF uptake Benefit: Mitigation of CLF based grid disruptions due to cyber security requirements	**Positive**
Any significant or adverse distributional impacts?	No	**Neutral**

(2) Expected impacts on businesses		
Description of overall business impact	Introduction of minimum customer protection and cyber security standards will level the playing field in the nascent load control market and preserve consumer confidence in CLF. Cyber security requirements will protect all businesses in GB from grid disruptions. However, FSPs and LCs will have to comply with the licence resulting in new costs to business and a new barrier to market entry.	**Positive**
Monetised impacts	Benefits were not monetised. Present value costs to business: £42m-£108m (2025 prices) Some of these costs will be passed through to households, mainly those who own ESAs and engage in load control (not quantified).	**Negative** **Based on likely business £NPV**
Non-monetised impacts	Benefit: FSPs and LCs will benefit from a larger load control market, enabled by increased consumer confidence delivered by the licence. Benefit: All GB businesses will benefit from less grid disruption through better cyber security standards in the load control market. Cost: Standardisation of load control activities can potentially hamper new business models and innovation.	**Positive**
Any significant or adverse distributional impacts?	Many of the management and customer protection requirements ask for business practices that are often already more established in large companies. Small and micro businesses often still have to adopt these. Therefore, based on the evidence obtained through the 2024 consultation, there is a trend that the additional costs are higher for small and micro businesses. However, these are both areas where the	**Negative**

	2024 consultation only covered high level policy proposals and did not include details of the proposed licence conditions underpinning company obligations and resultant costs. For example, a number of respondents explicitly referenced that the proposals were not sufficiently detailed to provide accurate cost estimates. We also made the decision to phase in consumer protections in the 2025 government response. We are seeking to validate the consumer protection and management cost assumptions through consultation questions 15 and 30. After acquiring more robust cost evidence, government will determine whether additional policy intervention may be required to mitigate the possible risk to small and micro businesses.	

(3) Expected impacts on households		
Description of overall household impact	All households will be able to benefit. Households owning ESAs and engaged in load control will be better protected from customer harms and cyber security attacks. The support of CLF more widely through load control will lead to a more efficient electricity system which benefits all consumers, including those households that do not engage in load control. The compliance costs for future licensees may lead to higher prices or less attractive load control offers for ESA owning households due to assumed passthrough costs.	**Positive**
Monetised impacts	NA	**Neutral**
Non-monetised impacts	See overall household impacts	**Positive**
Any significant or adverse distributional impacts?	No	**Neutral**

Part B: Impacts on wider government priorities

Category	Description of impact	Directional rating

Business environment: **Does the measure impact on the ease of doing business in the UK?**	Levelling the playing field and supporting consumer confidence will help grow the load control market, resulting in more opportunities for load control businesses to generate revenues. Though, the introduction of mandatory customer protection and cyber security requirements creates a new barrier to market entry. Standardisation of load control business practices may hamper innovation.	**Uncertain**
International Considerations: **Does the measure support international trade and investment?**	Not applicable.	**Neutral**
Natural capital and Decarbonisation: **Does the measure support commitments to improve the environment and decarbonise?**	CLF and load control are crucial to meet the Governments Clean power 2030 and Net Zero 2050 targets. CLF and load control, in particular, can help to balance the electricity system when it is dominated by intermittent renewables generation.	**Supports**

8. Monitoring and evaluation of preferred option

The introduction of the new load control licence will be accompanied by a robust monitoring and evaluation regime. To continually track the outcomes of the licence a range of monitoring sources is gathered.

The load control licence is part of the Smart Secure Electricity Systems programme (SSES). The SSES monitoring dashboard, which is owned by DESNZ, tracks 15 indicators capturing the impacts and wider outcomes of SSES deliverables according to the SSES theory of change. The data is mainly supplied through the Smart Systems monitoring dashboard and is updated annually.

Ofgem will be monitoring compliance with licence conditions and have access to cyber security incident reporting. Through the licence Ofgem would have the power to request information from licensees, which will be the main source of monitoring data. Ofgem also runs a regular survey (Flexibility and Net Zero survey (FANZ)) that captures, among others, wider outcomes of the licence.

Two evaluations are planned. A process evaluation will be conducted in 2028 after the introduction of the licence conditions appraised in this document. The objective is to assess the implementation process to draw lessons for the introduction of potential new licence conditions. The load control licence is part of SSES programme and will be a crucial part of the SSES impact evaluation carried out in 2031 when the whole programme is concluded.

9. Minimising administrative and compliance costs for preferred option

Policy and implementation details of the new licensing regime are still being developed. The responses to the consultation this document is a part of as well as a separate implementation-focused consultation by Ofgem will contribute an implementation approach that is cognisant of compliance and administrative costs for future licensees.

Summary: Analysis and evidence

For Final Stage Impact Assessment, these sections will be finalised including the full evidence base. Please note that we are uncertain about the evidence the net present social value findings are based on, given that a large proportion of the evidence comes from responses to our 2024 consultation covering high level policy proposals (see “4.2.2 Costs to Business” section for more detail). A number of respondents explicitly referenced that the consultation proposals were not sufficiently detailed to provide accurate cost estimates. We are therefore seeking to validate the cost assumptions through targeted questions in this consultation, which now includes a full draft licence.

Price base year: 2025

PV base year: 2025

	1. Do Nothing	**2. Load control licence with tiered cyber security requirements**	**3. Load control licence without tiered cyber security requirements**
Net present social value	Benefits: None Costs: £0	Benefits: Not monetised. Costs: £54m - £121m PV Cost arise predominantly from licensees complying with management controls, customer protection and cyber security requirements.	Benefits: Not monetised. Costs: £66m - £128m PV Cost arise predominantly from licensees complying with management controls, customer protection and cyber security requirements.
Public sector financial costs	None	Ofgem estimated costs: £13m PV	Ofgem estimated costs: £13m PV
Significant un-quantified benefits and costs	None	Support of CLF uptake through higher consumer confidence enabled by mitigation of customer protection. Protection of the electricity grid through higher cyber security standards. Tiered cyber security requirements ensure manageable costs for small and medium load LCs.	Support of CLF uptake through higher consumer confidence enabled by mitigation of customer protection. Protection of the electricity grid through higher cyber security standards. Untiered cyber security requirements create additional costs for small and medium LCs without significant increase in security benefits.
Key risks	NA	Potential upward sample selection bias in assumptions resulting in potentially overly conservative cost estimates.	Potential upward sample selection bias in assumptions resulting in potentially overly conservative cost estimates.

Results of sensitivity analysis	NA	Sensitivities represent degree to which licensees need to implement organisational changes (additionality). High estimates are more than twice higher than Low estimates representing the great uncertainty of total costs depending on the readiness of future licensees.	Sensitivities represent degree to which licensees need to implement organisational changes (additionality). High estimates are more than twice higher than Low estimates representing the great uncertainty of total costs depending on the readiness of future licensees.

Evidence base

1 Rationale for intervention

1.1 Background

Moving to a smarter and more flexible energy system is crucial for delivering the government's Clean Energy Superpower mission.[12] Great Britain (GB) increasingly needs sources of low carbon flexibility to facilitate a move away from a carbon-intensive system, in which unabated gas plays a major role in providing security of supply and electricity is generated by a small number of large power stations.[13] GB electricity demand is expected to increase significantly, due to the electrification of heat and transport sectors,[14] and supply of that will be through large quantities of intermittent renewables. System flexibility will be vital for shifting demand away from peak periods and utilising clean electricity when it is abundant, thereby ensuring the most cost-efficient system.

Low carbon flexibility can be provided by a range of sources, such as batteries, long duration electricity storage and consumer-led flexibility (CLF). CLF refers to actions taken by consumers to shift the time of their electricity use, typically to save money by accessing electricity at cheaper times of the day or to gain value from providing flexibility to others. CLF differs from energy efficiency and demand reduction, both of which involve reducing total demand rather than shifting demand to economically more optimal times, or to times when less stress is placed on the grid.

Consumer led flexibility (CLF)

A central subcategory of CLF is "load control", where an organisation directly controls the electricity consumption of an Energy Smart Appliance (ESA)[15] in line with market conditions to generate savings and revenue for the ESA owner. In the electricity system, load control is carried out by Flexibility Service Providers (FSPs) and Load Controllers (LCs). They connect consumers and their appliances to electricity markets. FSPs are consumer facing organisations that contract with consumers to shift electricity consumption and remunerate them for it. LCs remotely aggregate and control consumer appliances (through sending direct signals to the ESA) in line with their preferences and electricity market opportunities to earn revenues. It is also possible for organisations to operate in both roles.

The number of households and appliances controlled through FSPs and LCs as well as the corresponding CLF capacity provided to the grid is rising. In 2024, according to the National Energy Systems Operator (NESO), there was 1.6 GW of consumer-led flexibility utilised in GB (not including electric storage heater flexibility), with 0.2 GW coming from smart heat pumps and flexible district heating, 0.2 GW from EV smart charging, 0.3 GW from other smart appliances and 0.8 GW from non-domestic consumer-led flexibility.[16] With the further take-

[12] GOV.UK, 'Make Britain a Clean Energy Superpower'

[13] The National Energy System Operator (NESO) estimates that in 2024 around 50% of all electricity was produced using carbon-based fuels. NESO, 'Britain's Electricity Explained: 2024 Review'

[14] Currently, GB national demand is 330 TWh per annum. Depending on how we reach net zero, demand is expected to increase to between 450-500 TWh by 2035 and between 570-770 TWh by 2050. GOV.UK, 'Electricity networks strategic framework' (viewed on 8 December 2025)

[15] In the context of the load control licence only appliances which can shift significant loads are referred to as ESAs such as EV charge points, domestic batteries as well as electric heat appliances.

[16] NESO, 'Future Energy Scenarios' (viewed on 8 December 2025)

up of Energy Smart Appliances (ESAs) and a larger number of flexibility service offerings, there is considerable growth potential led by a broader base of consumers.[17] Based on NESO and DESNZ scenarios for 2030, we expect to enable 10-12GW of consumer-led flexibility capacity (excluding electric storage heaters) by 2030 to support clean power.

1.2 Problem under consideration

Increasing consumer engagement in CLF creates **cyber security and consumer protection risks**.

Cyber security: LCs will be able to remotely control significant amounts of electrical load through EV chargepoints, heat pumps etc. Without proper cyber security protections, an attack on a large number of devices, organisations, or supporting platforms could have serious consequences. An attacker that seizes control of many devices – or the systems used by organisations to control them – would be able to freely shift large volumes of demand up or down. If the amount of demand they control is large enough, they could cause damage to critical national infrastructure (CNI), with a consequent interruption of electricity supply to consumers that could potentially cause harm to life where consumers are critically dependent on that electricity supply. NESO estimates that an unplanned and sudden shift in 300MW of electrical load, via a cyber-attack, at times when the grid is under stress (for instance a calm, cloudy winter afternoon) could trigger blackouts. Potentially, attacks involving much smaller amounts of load could impact local infrastructure, e.g. causing the fuse at a local substation to 'trip'. Some organisations already control well above this level of electrical load, and, unlike traditional actors in the energy sector (such as unabated gas generators and DNOs), they are not currently subject to oversight or regulatory requirements to provide assurance that appropriate cyber security protections are in place.

Cyber-attacks on the energy sector are a real threat today. In the "Cyber security breaches survey 2025" approximately 70% of medium and large businesses stated that they were subject to a cyber-attack in the last 12 months.[18] The energy sector is the main target of attackers.[19]

Consumer protection: Poor consumer treatment leads to low levels of consumer trust which is essential to ensure mass uptake of CLF. With new companies entering a growing but unregulated CLF market, the risk of "bad actors" entering, who are unable or unwilling uphold consumer protection standards, rises too. New types of flexibility services and products come with potential risks of mis-selling or contractual obligations that "lock-in" consumers to using devices or services (like the early days of mobile phones when consumers faced barriers to switching mobile service operators). Further, there is a risk that consumers could purchase an expensive device and then find they receive poor quality service but are unable to change their service provider unless they replace the device.[20]

[17] Ofgem's State of the market report shows that between January 2024 and January 2025 the number of households using time of use tariffs grew by 70% from approximately 400,000 to 660,000. Ofgem, 'State of the energy market report: retail'

[18] GOV.UK, 'Cyber security breaches survey 2025'

[19] According to IBM's X-Force Threat Intelligence Index 2024 the UK energy sector is main target of cyber attackers in recent years. IBM, 'The UK energy sector faces an expanding OT threat landscape'

[20] This was the case with the first generation of smart meters (SMETS1), which often lost their smart functionality when customers switched energy supplier due to not being interoperable between different energy suppliers.

1.3 Potential market failures

Cyber security: Without additional regulation, firms may underinvest in cyber security[21] or other measures to address grid stability, which could have significant impact, due to the existence of the following market failures:

- **Externalities**: Firms may not fully capture the wider societal benefits of investing in cyber security or grid stability, as this exceeds their private benefit. This is because grid stability is a **public good**, where the benefits of security or stability are experienced by society as a whole, and network operators in the form of a more stable and lower cost energy system. These benefits are non-rivalrous and non-excludable.[22] Equally, the costs of insecurity or instability are also borne by the system. Therefore firms, have an incentive to **free ride,**[23] as they operate insulated from these benefits/costs which reduces their incentive to invest. Organisations primarily view risks to themselves, and not the system, which creates problems when smaller organisations become connected, creating points of vulnerability in the wider system.
- **Imperfect information:** Firms may not be sufficiently equipped to identify, understand, and implement sufficient cyber security or grid stability solutions as they do not fully understand the risk they present to the wider energy system. In addition, firms subject to cyber-crime may not report or may want to play down the severity of cyber security attacks to avoid potential reputational damage and associated financial impact. The aggregate impact of many load controlling devices optimising across the same time of use tariff could cause greater grid instability. However, individual organisations are unlikely to have the necessary information to be aware of this.

Consumer protection: Without government intervention, the following market failures are likely to arise which would prevent interoperability being achieved. Consequently, consumers may be 'locked in' when their preferences or circumstances change, or 'locked out' from better offers, impacting the growth potential of the CLF and ESA markets.

- **Market power** – A firm with a large market share or cost advantage may deliberately prevent rival firms from being interoperable with its products or services, to sell more products or maintain services over a longer period. Alternatively, firms with market power may develop interoperability solutions that favour their specific business, creating barriers to firms offering innovative approaches. Network effects may lead to this issue growing over time.[24]

[21] These risks are informed by the academic literature, for example a NATO CCDCOE Project Report, and a DSIT Impact Assessment on cyber security for consumer products, with both concluding the same market failures. NATO Cooperative Cyber Defence Centre of Excellence, 'Economic aspects of national cyber security strategies - Project Report' (viewed on 8 December 2025), and GOV.UK, 'Regulation of consumer connectable product cyber security – Impact Assessment' (viewed on 8 December 2025)

[22] Non-rivalry suggests the benefit one energy market participant receives from having a stable grid does not reduce the amount of benefit another can receive from having a stable grid. Non-excludability suggests that all energy market participants receive the benefit of a stable grid.

[23] The free rider problem is the burden on a shared resource that is created by its use or overuse by people who aren't paying their fair share for it or aren't paying anything at all.

[24] Network effects here means that the more customers that use a particular interoperability standard, the greater the value for that interoperability standard.

- **Coordination failure** – Firms may not have the incentive, capability or mechanisms to effectively co-ordinate to deliver interoperability.
- **Externalities** – The benefits to the energy system and consumers from maximising uptake of flexibility could be greater than the private benefit a firm perceives for investing in CLF, leading to a tendency to underinvest. This may be more prevalent in early markets for CLF services, where there may be little incentive for companies to invest additional time and energy in standardisation of products.

Consumers may also be exposed to the mis-selling of services due to:

- **Information asymmetry –** Consumers may face barriers to fully understanding the benefits and risks from engaging with ESAs and services involving CLF. This risk is particularly acute for CLF services, given the potentially complex arrangements needed between consumers and FSPs. Vulnerable consumers may be particularly exposed.

Without government intervention these risks will not be mitigated and overtime translate into consumer detriment and real economic damage. The 2019 Cyber Security Incentives and Regulation Call for Evidence found that 71% of respondents agreed that a lack of strong commercial rationale was a barrier for effective cyber risk management.[25] The 2025 Cyber Security Breaches Survey found that there is a clear lack of commercial interest in some companies to effectively negotiate a cyber security budget against other competing organisational priorities. The National Cyber Security Centre (NCSC) has also emphasised the need for intervention in the flexibility markets to mitigate cyber risk and has highlighted cyber proliferation and cyber threats to CNI as a key risk in its latest annual review.[26]

In terms of consumer protection, the energy supply market is a useful case study. Here Ofgem has to intervene every year to protect consumers from mistreatment from suppliers.[27] Consumers who engage in CLF to the benefit of the whole system also need protection. In the absence of this, consumers could lose trust in taking up these services risking the delivery of the Government's CLF ambition.

2 Policy objective

By implementing the load control licensing regime, government wants to meet the following objectives:

1. By 2028 enabling increased uptake of domestic and small non-domestic CLF through giving consumers confidence to engage with a smart energy system and create a level-playing field for participating companies.
2. By 2028 reducing the cyber security and grid stability risks to our electricity system resulting from the increased uptake of domestic CLF.

The licensing regime will ensure that LCs are cyber and grid-secure and FSPs protect their consumers. This will contribute to consumer trust in CLF and mitigate CLF related risks to the electricity system. Alongside other enabling policies this will lead to higher consumer

[25] GOV.UK, 'Cyber Security incentives & regulation review: government response to the call for evidence' (viewed on 8 December 2025)
[26] NSCS, 'NSSC Annual Review 2024' (viewed on 8 December 2025)
[27] Ofgem, 'Enforcement cases' (viewed on 8 December 2025)

engagement with CLF to provide low-cost and zero-carbon flexibility to the electricity system. This directly supports the HMG objectives of making the UK a clean energy superpower.

3 Options

3.1 Long list appraisal

Government considered the following long list of options to deliver the objectives:

- Option I: Do Nothing - Voluntary, industry led standards
  In a "Do Nothing" scenario FSPs and LCs would manage their consumer relations and cyber security according to their requirements. They may choose to accede to voluntary, industry led standards where these exist.

- Option II: Load control licence
  Government would create a new licence for organisations involved in load control services in order to protect consumers and the electricity system from unacceptable risks associated with the control of ESAs for CLF. To create this licence, government will need to pass secondary legislation and draft licence conditions. Ofgem, as with other electricity system licences, will be the regulating authority for the new licence. Consumer protection and cyber security measures could be tiered leading to the following sub options.

    - Option IIa) Tiered consumer protection
      To soften the administrative burden on small and medium sized businesses, the consumer protection and cyber security requirements would be tiered. FSPs with fewer consumers below a certain threshold would be subject to softer requirements. For LCs a basic and an enhanced tier of requirements would be introduced depending on the level of load they control.

    - Option IIb) Tiered cyber security
      To manage the administrative burden on smaller LCs and to scale cyber security protections in line with risk, a basic and an enhanced tier of requirements would be introduced. One set of consumer protection requirements for all FSPs.

    - Option IIc) Untiered licence
      All licensees would follow the same consumer protection and cyber security requirements.

- Option III: Load control licence + a new load control industry code
  In addition to the load control licence, a new industry code could be established between relevant industry parties (e.g., FSPs, Load controllers, suppliers, grid operators) administered with a new code manager licenced by Ofgem. This code could cover a variety of business-to-business arrangements to support domestic CLF. For example, agreed industry best practices on consumer communication around CLF, and arrangements on how a FSP and supplier interact when they are both supplying services to the same property.

To assess the suitability of the long list options, the following critical success factors were employed.

1. Strategic fit. Is the option suitable to deliver the objectives of 'Enabling increased uptake of domestic CLF' and 'Reducing the grid stability and cyber security risk arising from the increased uptake of domestic CLF'?
   Domestic CLF is a nascent market. Many FSPs currently operate with small profit margins. To grow the domestic CLF market, regulations need to strike the right balance to encourage an expansion of CLF services and ensure integrity of the system whilst avoiding any undue cost burdens for businesses.

2. Value for money. Is the option suitable to deliver the programme objectives at the least cost to business?
3. Affordability Is the option suitable to deliver the programme objectives at the least cost to the tax- or bill payer?
4. Achievability. Is the option deliverable and can be implemented in a timely way to achieve objectives?

The detailed appraisal of the long list options can be found in the Appendix in Table 21. Table 1 shows a summary.

Table 1: Summary of long list appraisal, Option 2b is the preferred option

Long list Options	Strategic fit	Value for money	Affordability	Achievability
Option I	☒	☑	☑	☑
Option IIa	☒	•••	☑	•••
Option IIb	☑	•••	☑	•••
Option IIc	•••	•••	☑	•••
Option III	•••	•••	☑	☒

Voluntary standards leave an excessive risk of consumer harm or grid disruption. Hence, Option I was excluded due its poor strategic fit, though it is also the counterfactual in the short list appraisal. Introducing a new industry code would risk stifling innovation in a nascent market and would be very complex and time consuming to implement. Hence, Option III was excluded due to weak strategic fit and poor achievability.
The preferred option is a load control licence (Option II). As set out in more detail in Table 21 tiering of consumer protection requirements was deemed to undermine the core objective of the licence. Tiering of cyber security requirements (Option IIb) is the governments preferred option because in this option the requirements are tailored to the cyber security risk an organisation creates to the system. Tiering consumer protections is undesirable because consumers need to be equally protected across the market for them to have confidence in it.

3.2 Short list

Following the long list appraisal, government considered the following short list of options.

- Option 1: Do Nothing - Voluntary, industry led standards
  In a Do Nothing scenario FSPs and LCs would manage their consumer relations and cyber security according to their requirements. They may choose to accede to voluntary, industry led standard where these exist.
  This option serves as counterfactual in the short list appraisal.

- Option 2: Load control licence with cyber security tiering (preferred option)
  Government would create a new licence for organisations involved in load control services in order to protect consumers and the electricity system from unacceptable risks associated with the control of ESAs for CLF. Ofgem, as with other electricity system licences, will be the regulating authority for the new licence. To manage the administrative burden on smaller LCs and to scale cyber security protections in line with risk, a basic and an enhanced tier of requirements would be introduced. One set of consumer protection requirements would apply to all FSPs, and would be phased in over time, with the first set representing a minimum standard of acceptable protection. Long list options 2a) and 2c) are excluded from the short list appraisal. Both options failed to meet the strategic fit criteria in the long list appraisal. Full details can be found in Table 21.

- Option 3: Untiered Load controlled licence
  As in option 2, government would create a new licence for organisations involved in load control services. All licensees would follow the same consumer protection and cyber security requirements.

3.3 Preferred option

The preferred option is to introduce a new Load Control Licence with tiered cyber security requirements administered and enforced by Ofgem (option 2). In the 2025 SSES government response, we also confirmed that we would phase consumer protection requirements and only subject organisations to licence requirements based on their applicability to the activity they undertake.

We are therefore proposing the new load control licence will comprise 14 licence conditions, which can be reviewed in detail in the draft licence conditions published alongside this consultation. The new licence will have two sub-categories, one for FSPs and one for LCs. Table 2 below provides a summary of all licence conditions, their applicability to FSPs or LCs as well as cost categories we will use for the remainder of this document to structure the appraisal.

To ensure that LCs meet proportionate cyber security requirements the preferred option intends to use the Cyber Assessment Framework (CAF), a tool developed by the National Cyber Security Centre (NCSC) as an outcomes focused framework to assess cyber resilience. The implementation of the CAF is the main distinguishing factor between short list options 2 and 3. The distinction is set out below.

- Two bespoke CAF profiles will be developed – a ‘tier 1’ profile for large load controllers (>300MW), and a ‘tier 2’ profile for load control licensees managing <300MW load.
- **Tier 1:** Load controllers who manage equal to or above 300MW of load (Large Load Controllers – LLCs) will need to hold a licence but their cyber security will be

regulated via the Network and Information Systems (NIS) Regulations 2018, in line with other 'Operators of Essential Services'.

- **Tier 2:** Load controllers who manage below 300MW are in scope of the load control licence, and will be required to adopt requirements modelled on NIS through the licensing framework.

Ofgem will deliver the load control licence and is consulting on the implementation process in their "Smart Secure Electricity Systems: Implementing the load control licensing regime" consultation. Government and Ofgem aim for new licensees to be able to apply by the end of 2026 and for the requirement to hold a licence to be in force by the end of 2027.

Table 2: Licence conditions, applicability and appraisal cost categories

#	Licence Condition	FSPs	LCs	Cost category
1	Definitions for standard conditions	☑	☑	General
2	Interpretation of standard conditions	☑	☑	General
3	Operational capability	☑	☑	General
4	Financial responsibility principle	☑	☑	Management controls
5	Ongoing fit and proper requirement	☑	☑	Management controls
6	Provision of Information to Authority and Secretary of State	☑	☑	Data provision
7	Principle to be open and cooperative	☑	☑	General
8	Requirement to comply with industry codes	☒	☑	Code compliance
9	Cyber assurance framework for load controllers	☒	☑	Cyber security
10	Load control check	☒	☑	Cyber security
11	Treating Customers Fairly	☑	☒	Customer protection
12	Recommending suitable services and prohibiting mis-selling	☑	☒	Customer protection
13	Allow customers to exit a service	☑	☒	Service Exit
14	Requirement that fees charged by FSPs which are associated with a customer's service exit must be proportionate	☑	☒	Service Exit

4 NPSV: monetised and non-monetised costs and benefits of each shortlist option (including administrative burden)

4.1 Benefits

The new load control licensing regime will significantly support consumer confidence and cyber security in CLF market. It has not been possible to quantify and monetise these benefits for this document.

4.1.1 Consumer confidence benefits

Stronger consumer confidence is highly likely to lead to an increase in CLF uptake and higher flexibility capacity to the system. More system flexibility translates into cost savings for the system due to lower capital costs for generation and network infrastructure. This will result in lower consumer bills. The total benefit of CLF to the UK electricity system has been

estimated by the Electricity Networks Strategic Framework analysis (ENSF) to be £40-50bn (cumulative, 2021-2050, 2020 prices).[28] This should translate into savings for all households, including those who do not significantly shift their demand. Households who are able to shift their demand, through charging their EV at night for instance, can achieve additional bill savings.[29]

The load control licence, as well as the wider SSES programme, is an enabling policy. Higher CLF uptake is only achieved in line with complementary policies and developments such as Market Wide Half Hourly Settlements and Time-of-use-Tariff rollout. As such it is difficult to attribute to the licence the proportion of the monetary benefits that higher consumer confidence delivers. It is, however, clear that the benefits outlined above could not be achieved or would be at a great risk without the licence.

4.1.2 Cyber security benefits

As set out in more detail above, a significant increase in CLF and load control gives rise to a new cyber security risk. Attackers could exploit load controllers to destabilise the electricity system and attack Critical National Infrastructure. For example, cyber-attackers could seek to compromise through a load controller a large number of devices in order to simultaneously and repeatedly turn them on and off, which would cause significant challenges for the system operator in managing and balancing the grid. Soon there could be enough smart devices on the system that an attack of this type could feasibly cause local or national power outages (i.e. blackouts) in certain circumstances.

Historic large-scale blackouts, while not necessarily caused by a cyber-attack, offer us an indicative sense of scale of an attack of this nature. Some examples are outlined in Table 3 below.

Table 3: Indicative estimates of large-scale electricity network outages.

Example	Details	Indicative system cost	
Spain/Portugal 28 April 2025 [30] [31]	50m consumers affected for up to a day	€0.4bn-1.6bn (2025 prices)	£0.3bn-1.4bn (2025 prices)
UK: 9 August 2019 [32]	Over 1m consumers affected for up to an hour	£15m (2019 prices)	£19m (2025 prices)
2003 North America [33]	55m consumers affected for up to a few days	$6bn (2008 prices)	£5bn (2025 prices)
Cambridge 2016 analysis [34]	Scenario1: up to 9m consumers affected for up to 3 weeks	£12bn (2016 prices)	£16bn (2025 prices)

[28] GOV.UK, 'Electricity networks strategic framework' (viewed on 8 December 2025)
[29] Currently, an EV owner with an annual milage of 7,400m and access to an off-street charge point can save £332 off their electricity bill according the 2024 Default energy tariffs for households; call for evidence. GOV.UK, 'Default energy tariffs for households: call for evidence' (viewed on 8 December 2025)
[30] CaixaBank Research, 'The economic impact of the blackout in detail' (viewed on 8 December 2025)
[31] Reuters, 'Post-blackout in Spain and Portugal, companies count the cost' (viewed on 8 December 2025)
[32] Drax, 'Electric Insights Quarterly Reports – The Blackout' (viewed on 8 December 2025)
[33] Onyx Impact, 'The Blackout Impact' (viewed on 8 December 2025)
[34] Cambridge Centre for Risk Studies, 'Cambridge Risk Framework for Critical Infrastructure Threat Scenario, Integrated Infrastructure: Cyber Resiliency in Society - Mapping the Consequences of an Interconnected Digital Economy' (viewed on 8 December 2025)

The cybersecurity measures included in the licence aim to minimise these potential costs. However, the uncertainty around the likelihood and severity of cyber-attacks in the future mean cyber security benefits cannot be accurately forecasted. Break-even analysis, however, can provide some insights.

How many households, and for how long, would need to be affected by a disruption for the cost of preventing it through the cyber requirements in the licence to be justified? The full method is set out in the Appendix to this document. The results in Table 4 show total discounted cyber costs over the ten-year appraisal period are equivalent to the economic damage from 602MWh to 1000 MWh for Option 2 and 1085MWh to 1276MWh for Option 3.

Table 4: Cyber Benefits - Break-even load loss

Break even load loss (MWh)	Option 2	Option 3
Low	602	1085
Central	791	1181
High	1000	1276

Based on the average annual household consumption in the UK,[35] this is equivalent to 0.25% to 0.41% of households losing electricity for one day in Option 2 (0.45% to 0.53% in Option 3) in one instance in the next 10 years. This shows that a one-day interruption of supply for less than 1% of households is worth the costs of the cyber protection requirements. One can extrapolate this to conclude that the damage of even a short national blackout would vastly exceed the cyber costs of the licence for both options.

Table 5: Cyber benefits – Break-even household supply interruption

	Days of interrupted HH supply (thousands)		Share of UK households with 1 day of interrupted supply	
	Option 2	Option 3	Option 2	Option 3
Low	71	128	0.25%	0.45%
Central	93	139	0.33%	0.49%
High	118	151	0.41%	0.53%

Break even analysis is unsuited to distinguish the cyber security benefits of Options 2 and 3. In Option 3, small and medium sized load controllers would have to follow the same stringent cyber security requirements as large load controllers. In Option 2 small and medium sized LCs would follow adjusted requirements.

The benefit of cyber security measures is the reduction impact and likelihood of future attacks and the resulting grid disruptions. The impact and likelihood of a successful cyber attack on a LC correlates to the level of load controlled. A successful attack on a large LC creates more damage than an attack on a small or medium LC. This makes large LCs a more attractive target and more likely to be attacked. Hence, small and medium sized load controllers present a smaller security risk to the UK system.

[35] The average household electricity in the UK in 2024 was 3,090 MWh. GOV.UK, '[Average annual domestic electricity bills by various consumption levels (QEP 2.2.5)]' (viewed on 8 December 2025)

Requiring that small and medium sized LCs follow the same standards as large LCs, despite their cyber risks being lower is not proportional. The additional security benefits of more stringent measures for small and medium LCs would not lead to significant reductions in attack impact or likelihood as these LCs are a lot less likely to be attacked in the first place. One could say, their lower size a kind of cyber protection already.

4.2 Costs

4.2.1 Appraisal Methodology

First the compliance costs per individual licensee are estimated. These are then aggregated to estimate the total costs to business. The costs to Ofgem are also estimated. The total social costs comprise the costs to business and the costs to Ofgem. Table 6 sets out the cost categories used to appraise the cost per individual licensee.

Table 6: Appraisal overview of licence cost categories

Cost category	Appraisal
General	No additional costs – assumption tested via consultation
Code compliance	Monetised
Management controls	Monetised
Data provision	Indicatively monetised
Grid Stability	Monetised
Cyber security	Monetised
Customer protection	Monetised
Service Exit	Not monetised - requested data via consultation

As set out in section 3.2 Option 1, Do Nothing, serves as a **counterfactual.** All cost calculations below show the relative difference in costs between compared to Option 1.

In addition to the central scenario, a high and a low **sensitivity** have been modelled. These sensitivities represent additionality or the degree to which companies have to implement changes to comply with the new licence. Where possible costs are estimated separately for different company sizes.

An optimism bias assumption of 10% has been applied during the aggregation of total costs. This is based on the lower bound of Equipment/Development projects in the Green Book supplementary guidance on optimism bias.[36] The lower bound was selected because evidence in this assessment is based on stakeholder consultation and because of the robust project and risk management structures. Both factors are quoted in the guidance as potential ways to reduce optimism bias.

We are aiming for applications for the licence to open by the end of 2026 and to be enforced by the end of 2027, 12 months after applications open (subject to the outcome of question 7 in the consultation). Ofgem is already preparing this launch now and incurring

[36] GOV.UK, '[Green Book supplementary guidance: optimism bias]' (viewed on 8 December 2008)

costs for additional staff. Hence, the **appraisal period** is set to start in 2025 and spans to 2034 to cover a standard period of 10 years.

4.2.2 Costs to Business

4.2.2.1 Management controls

Management controls comprise the ongoing fit and proper requirement for managers and the financial responsibility principle. The former requires that licensees must ensure, on an ongoing basis, that their senior personnel are suitable to occupy that role, and requiring that licensees must have robust processes, systems and governance in place to ensure this. The condition also requires that regular assessments are carried out to ensure personnel remain 'fit and proper'. The financial responsibility principle is a requirement for licensees to ensure that licensees maintain sufficient capital and liquidity that they are able to meet their reasonably anticipated financial liabilities. It also includes a requirement to proactively disclose signs of financial distress.

The assumptions to estimate the costs of the requirements to licensees are based on the responses to the 2024 SSES licensing consultation (Question 48).[37] Unfortunately, very few respondents gave quantitative estimates. Hence the sample, especially considering different company sizes, is small and the assumptions should be treated with caution. Furthermore, the 2024 consultation covered high level policy proposals and did not include details of the proposed licence conditions underpinning company obligations and resultant costs. A number of respondents also explicitly referenced that the proposals were not sufficiently detailed to provide accurate cost estimates. Little detail was included on Ofgem's approach to administering the licence obligations, which also has an impact on the costs to companies. Ofgem are publishing a consultation on their approach to implementing the licensing regime in parallel to this consultation.

Nonetheless, the responses show a trend that small companies face higher costs than medium or large companies. This is due to large companies having to fulfil many of the obligations in these licence conditions already anyway and therefore will only have to implement few or no additional changes. The full set of assumptions is shown in Table 7. Management control costs are the same for Options 2 and 3. Due to small sample size, we were unable to derive High/Low sensitivities. Government are seeking to validate or improve these assumptions through consultation question 15.

Table 7: Management Controls, annual costs per licensee assumptions, Option 2 and 3

Management Control Costs (2025£)	Company Size		
	Small	Medium	Large
Annual costs	98,000	49,000	12,000

4.2.2.2 Data Provision

This draft condition requires licensees to provide Ofgem with information essential for monitoring and compliance. It will enable Ofgem to carry out monitoring activities and provide insight into any emerging consumer harms that may arise in the market as it develops.

[37] GOV.UK, 'Consultation outcome. Delivering a smart and secure electricity system: implementation' (viewed on 8 December 2025)

Through question 15 in Ofgem's consultation document the government and Ofgem hope to obtain the accurate costs of this requirement. In the interim a proxy from 2021 Ofgem consultation on Consolidated Segmental Statements was used for this appraisal.[38] The detailed assumptions are shown in Table 8. Data provision costs are the same for Option 2 and 3.

Table 8: Data provision, annual costs per licensee assumptions, Option 2 and 3

Data Provision Costs (2025£)	Sensitivity		
	Low	Central	High
Annual costs	7,300	15,700	24,200

4.2.2.3 Code compliance

The draft condition requires that load controllers have to accede to the Balancing and Settlement Code (BSC) to contribute to the ongoing governance of the SSES programme through Elexon, the current code administrator. Sign-up and monthly fees for load control licensees have not been set up yet. Hence, we take the costs for electricity suppliers as a proxy. These are £500 for acceding to the BSC and a monthly fee of £250+VAT.[39] Code compliance costs are the same for Options 2 and 3.

Table 9: Code compliance, cost per licensee assumptions, Option 2 and 3

Code Compliance costs (2025£)	
Set Up (Year 1)	£4,100
Ongoing (Year 2ff)	£3,600

To achieve and maintain stability of the electricity network and the electricity grid when third parties are undertaking load control, government and Ofgem want to include a condition within the load control licence requiring that a load controller must comply with (and where relevant accede to) the following codes:

- The Grid Code
- The Distribution Code
- Connection and Use of System Code (CUSC)
- Distribution Connection and Use of System Agreement (DCUSA)

The Grid Code and the Distribution code are contractually enforceable through CUSC and DCUSA respectively. Hence, the cost implication of this licence conditions arises from acceding to CUSC, which costs £3,600 per year.[40] Acceding to DCUSA is free. Grid stability costs are the same for Option 2 and 3.

Table 10: Grid Stability, annual costs per licensee assumptions, Option 2 and 3

Grid Stability costs (2025£)
Acceding to CUSC

[38] Ofgem, 'Final proposals and statutory consultation - Reviewing the Consolidated Segmental Statement', page 51 (viewed on 8 December 2025)
[39] Elexon, 'Becoming a Supplier' (viewed on 8 December 2025)
[40] Acceding to CUSC costs £3000+VAT.

Set Up (Year 1)	£3,600

4.2.2.4 Cyber Security

To ensure that LCs meet proportionate cyber security requirements the government and Ofgem intend to use the Cyber Assessment Framework (CAF), a tool developed by the National Cyber Security Centre (NCSC) as an outcomes focused framework to assess cyber resilience. The implementation of the CAF is the main distinguishing factor between short list options 2 and 3. The distinction is set out below.

Option 2 – Tiered cyber security requirements

- Two bespoke CAF profiles will be developed – a 'tier 1' profile for large load controllers (>300MW), and a 'tier 2' profile for load control licensees managing <300MW load.
- **Tier 1:** Load controllers who manage equal to or above 300MW of load (Large Load Controllers – LLCs) will need to hold a licence but their cyber security will be regulated via the Network and Information Systems (NIS) Regulations 2018, in line with other 'Operators of Essential Services'.
- **Tier 2:** Load controllers who manage below 300MW are in scope of the load control licence and will be required to adopt requirements modelled on NIS through the licensing framework.

Option 3 – Untiered cyber security requirements

- All load controllers need to hold a licence.
- **All load controllers** have to follow the **Tier 1** CAF profile, regardless of the volume of electrical load they control.
- Cyber security compliance for load controllers who manage equal to or above 300MW of load (Large Load Controllers – LLCs) will be regulated via the Network and Information Systems (NIS) Regulations 2018, in line with other 'Operators of Essential Services'.

The appraisal of the costs to licensees arising from cyber security requirements is based on the 2022 Post Implementation Review of the NIS regulations.[41] The main cost categories covered are: familiarisation costs, contract change costs, costs of incident reporting, compliance costs as well as security costs due to additional physical infrastructure and internal and external staff needed. They do not however, take into consideration any existing costs currently incurred by meeting other cyber security measures, for example ISO 27001 compliance. Therefore, these figures are likely an overestimate. Though there are differences in the type of companies in scope of the PIR and the future larger load controllers, the 2022 PIR estimate for NIS costs is still deemed to be the best proxy. Table 11 shows the full set of assumptions for load controllers subject to the tier 1 CAF profile. These apply to large load controllers in Option 2 and to all load controllers in Option 3. Although for both, Option 2 and 3, it is worth noting that the cyber costs of large load controllers are not included in the total costs to business or total social costs. This is

[41] GOV.UK, 'Second Post-Implementation Review of the Network and Information Systems Regulations 2018' (viewed on 8 December 2025)

because large load controllers are enforced through the NIS regime and the cost impacts are accounted for there. It is assumed that licensees that are also large companies are also large load controllers with control over more than 300MW.

Table 11: Cyber Security, annual cost assumptions, Tier 1 CAF profile

Tier 1 Load Controllers Cyber Costs (2025£)			Sensitivity	
Cost category	**Cost type**	**Low**	**Central**	**High**
Familiarisation with NIS	Set Up	1,200	1,200	1,200
Contract Change Costs	Set Up	300	1,700	3,400
Incident reporting	Ongoing	3	5	7
Compliance costs	Ongoing	400	400	600
Additional Security Costs - physical	Set Up	105,200	114,300	123,300
Additional Security Costs - external	Ongoing	92,200	100,300	108,500
Additional Security Costs - internal staff	Ongoing	89,000	96,700	104,400
Total	**Set Up**	**288,300**	**314,600**	**341,400**
Total	**Ongoing**	**181,600**	**197,400**	**213,500**

Given tier 2 of the CAF is less onerous than tier 1, the costs for LCs below 300MW will be lower than those shown in Table 11. To collect accurate data for the final stage licensing impact assessment question 24 in the main consultation document was included. To generate an estimate for this appraisal in the interim the costs for large load controllers are adjusted with a bespoke multiplier based on the proportion of partially achieved CAF outcomes in tier 2 vs tier 1.[42] It is shown in Table 12.

Table 12: Cyber Security, CAF Tier 1/2 multiplier

	Low	**Central**	**High**
CAF Tier 1/2 multiplier	0.55	0.67	0.78

The resulting cyber cost assumption for load controllers below 300MW, Tier 2, are shown in Table 13. These only apply for load controllers below 300MW in Option 2. It is assumed that small and medium sized licensees who are load controllers fall into this category.

Table 13: Cyber Security, annual cost assumptions, Tier 2 CAF profile

Tier 2 Load Controllers Cyber Costs (2025£)			Sensitivity	
Cost category	**Cost type**	**Low**	**Central**	**High**
Familiarisation with NIS	Set Up	700	800	900
Contract Change Costs	Set Up	200	1,100	2,700
Incident reporting	Ongoing	0	0	0
Compliance costs	Ongoing	200	300	400
Additional Security Costs - physical	Set Up	58,000	76,200	96,500

[42] The CAF profile for load controllers has 39 outcomes in total. To meet Tier 1 35 outcomes have to be fully achieved and 4 partially. To meet Tier 2 only 17 outcomes have to be fully achieved and 22 have to be partially achieved. To generate the multiplier it was assumed that every CAF outcome incurs the same cost of implementation and that partial achievement of an outcome reduces this cost by 50% in the central scenario (Low: 75%, High: 25%) compared to full achievement.

Additional Security Costs - external	Ongoing	50,800	66,900	84,900
Additional Security Costs - internal staff	Ongoing	49,100	64,500	81,600
Total	**Set Up**	**159,000**	**209,800**	**267,000**
Total	**Ongoing**	**100,100**	**131,700**	**166,900**

4.2.2.5 Customer Protection

Customer protection requirements for FSPs are designed to ensure that consumers have adequate assurances that they can confidently engage in the market. They also ensure a level playing field for FSPs. Government also believes that these requirements are critical to enabling Ofgem to have oversight of consumer protections in the load control sector, as well as enforcement powers to sanction licensees who fall short on expected minimum standards.

FSPs or representatives acting on their behalf are expected to:

- Behave and carry out actions in a fair, honest, transparent, appropriate and professional manner.
- Ensure they provide information to their customers that is clear, accurate and not misleading.
- Have adequate customer service arrangements in place that allow customers to easily contact the licensee and ensure that mistakes are rectified promptly and courteously.
- Seek to identify domestic customers in vulnerable situations and ensure that the vulnerable situation of any domestic customer is taken into account when the standards of conduct are applied.
- Make sure that only suitable services are recommended. For example, EV smart charging providers would be expected to enquire about their customers' charging schedule preferences before recommending an FSP service, to ensure its suitability.
- Not employ inappropriate mis-selling techniques, and make certain terms and conditions clear to consumer ahead of time of agreeing the contract.

FSPs will also have to offer complaints procedures and contribute to dispute resolutions. Legally this will not be achieved through the licence but through bringing FSPs within scope of statutory framework for complaints and dispute resolution regulation i.e. - Consumers, Estate Agents and Redress Act 2007,[43] The Gas and Electricity Regulated Providers (Redress Scheme) Order 2008,[44] and The Gas and Electricity (Consumer Complaints Handling Standards) Regulations 2008.[45] As part of this, FSPs will be required to participate in the Energy Ombudsman alternative dispute resolution scheme.

The assumptions to estimate the costs of the requirements to FSPs are based on the responses to the 2024 SSES licensing consultation (Questions 30 and 31).[46] The estimates

[43] Consumers, Estate Agents and Redress Act 2007 (viewed on 8 December 2025)
[44] The Gas and Electricity Regulated Providers (Redress Scheme) Order 2008 (viewed on 8 December 2025)
[45] The Gas and Electricity (Consumer Complaints Handling Standards) Regulations 2008 (viewed on 8 December 2025)
[46] GOV.UK, 'Consultation outcome. Delivering a smart and secure electricity system: implementation' (viewed on 8 December 2025)

should be treated with caution as the 2024 consultation covered high level policy proposals and did not include details of the proposed licence conditions underpinning company obligations and resultant costs. A number of respondents also explicitly referenced that the proposals were not sufficiently detailed to provide accurate cost estimates.

Area proposed in 2024 consultation	Carried forward into 2025 consultation?
General consumer protection condition	Yes
Recommending suitable services	Yes
Internal complaints procedures	Yes
Dispute resolution	Yes
Independent consumer advocacy and guidance	No
Identification and record-keeping of vulnerable situations	Identification but not formal record keeping
Inclusive and accessible design and communication	No
Consumer control over a load control DSR service	No

To develop cost estimates for this impact assessment we have, therefore, adjusted down the estimates provided in the responses by 40%. This is a policy assumption used to reflect the impact of a reduced scope for the licence conditions from those described in the last consultation. We anticipate receiving updated estimates from respondents to the 2025 consultation question 30 and 33, from which this analysis will be updated.

Furthermore, in the 2025 government response to the 2024 consultation, government decided to phase consumer protection requirements. Little detail was also included on Ofgem's approach to administering the licence obligations, which also has an impact on the costs to companies. Ofgem are publishing a consultation on their approach to implementing the licensing regime in parallel to this consultation. Government are seeking to validate or improve these assumptions through consultation question 30.

Nonetheless, there was a logical pattern in that respondents stating that they had already implemented some or many of the requirements reported low-cost estimates. Conversely respondents that stated they had to set up new activities, reported higher cost estimates. Hence, the estimates of the former group of respondents was aggregated to create the Low sensitivity while the estimates of latter group of respondents was used for the High sensitivity. The Central sensitivity is the average of the Low and High sensitivity. As set out before the High/Central/Low sensitivities represent additionality or the degree of companies' additional change needed to implement licence conditions. The full set of assumptions is shown in Table 14.

The cost evidence for small and medium companies was not significantly different. Due to the small sample size underpinning the assumptions it was not possible to generate separate assumptions for small and medium sized companies. The cost evidence for large companies was significantly different and significantly lower. As with management controls, it is likely that large companies with existing customer relationships already do many of the future requirements of the licence and hence have to introduce fewer changes than small or medium companies. The contrasting expectation that a smaller customer base would lead to less FTE requirements, such as needing less customer service staff, is not reflected in the evidence provided to date.

Another trend is observable. The difference between low and high-cost estimates is larger than the difference between cost estimates for small/medium and large companies. This shows that a crucial driver for customer protection cost is the extent to which companies have already implemented relevant activities. This applies particularly strongly to existing electricity suppliers as the customer protection requirements in the load control licence are designed to closely match those of the electricity supply licence. Only one supplier provided cost estimates in the 2024 licensing consultation, and it is telling they provided an estimate of zero.

Table 14: Customer Protection, annual costs per FSP assumptions

Customer Protection Costs (2025£)	Company Size	
	Small & Medium	Large
Low	34,000	0
Central	130,000	88,000
High	227,000	176,000

4.2.2.6 Service Exit

The load control licence includes the requirement to allow customers to exit an FSP service. There is also a requirement that any fees charged by FSPs, which are associated with a customer's service exit, must be proportionate as well as clearly communicated at the start of the contract between customer and FSP.

Through the permission for FSPs to charge an exit fee, the direct economic costs for FSPs can be transferred to consumers. Thus, this should not create additional costs for FSPs. The government and Ofgem are unaware of any further costs arising from these conditions. Nonetheless, question 33 in the main consultation document allows respondents to specify which cost should be considered in future appraisals.

4.2.2.7 Total costs to business

Table 15 and Table 16 below show the total costs per licensee for Option 2 and 3 respectively. For cyber security it is assumed that small and medium sized licensees fall below the 300MW threshold while large licensees are assumed to be also large load controllers. Large load controllers' cyber security will be enforced through the NIS regime. Given this document is appraising the impact of the load control licence, cyber security costs for large load controllers have been set to zero.

As mentioned above, a number of the cost estimates come from the 2024 consultation which only covered high level policy proposals and did not include details of the proposed licence conditions underpinning company obligations and resultant costs. Little detail was included on Ofgem's approach to administering the licence obligations, which also has an impact on the costs to companies.

Table 15: Total annual costs per licensee, Option 2, 2025£, thousands, L:Low, C:Central, H:High sensitivity

Costs per licensee (2025£k) **Option 2** (annual)		Small		Medium		Large	
		Set Up	Ongoing	Set Up	Ongoing	Set Up	Ongoing
Flexibility Service Providers	L	143	143	94	94	24	23
Flexibility Service Providers	C	248	248	199	199	120	119

Flexibility Service Providers	**H**	353	352	304	303	216	216
Load controllers	**L**	275	209	226	160	27	23
Load controllers	**C**	335	249	286	200	36	32
Load controllers	**H**	400	292	351	244	44	40
Combined	**L**	309	243	261	194	27	23
Combined	**C**	465	379	416	330	124	119
Combined	**H**	627	519	578	470	220	216

Table 16: Total annual costs per licensee, Option 3, 2025£, thousands, L:Low, C:Central, H:High sensitivity

Costs per licensee (2025£k) **Option 3** (annual)		**Small**		**Medium**		**Large**	
		Set Up	**Ongoing**	**Set Up**	**Ongoing**	**Set Up**	**Ongoing**
Flexibility Service Providers	**L**	143	143	94	94	24	23
Flexibility Service Providers	**C**	248	248	199	199	120	119
Flexibility Service Providers	**H**	353	352	304	303	216	216
Load controllers	**L**	405	290	356	241	27	23
Load controllers	**C**	439	315	391	266	36	32
Load controllers	**H**	475	339	426	290	44	40
Combined	**L**	439	324	390	276	27	23
Combined	**C**	570	445	521	396	124	119
Combined	**H**	702	566	653	517	220	216

To estimate the total costs to business, the cost per licensee needs to be multiplied by the forecasted number of load controllers. Government and Ofgem through their industry engagement have compiled a list of potential FSPs and LCs as well companies who fulfil both roles. A total of 45 potential companies have been identified that are likely to apply for a licence. Table 17 shows the resulting numbers that are used to calculate the total costs that are shown in Table 18. The number of potential licensees is the same for Option 2 and 3.

Table 17: Number of potential licensees, Option 2 and 3

Number of potential licensees	**Small**	**Medium**	**Large**
FSP only	8	2	6
LC only	3	2	4
Combined	6	6	8

Table 18: Total cumulative costs to business

Costs to business (2025£m, cumulative 2025-34, discounted)	**Option 2**	**Option 3**
Low	42	53
Central	75	84
High	108	115

4.2.3 Ofgem costs

Ofgem will administer and enforce the new load control licensing regime. To do this effectively Ofgem needs to hire additional staff. Ofgem has carried out an internal assessment of the additional needs, which informed the cost assumptions in Table 19. Ofgem cost are the same for Option 2 and 3.

Table 19: Ofgem annual costs assumptions, Option 2 and 3

Ofgem Costs (2025£m, undiscounted)	2025	2026-34
Annual Ofgem Costs	1.1	1.6

4.2.4 Total social costs

Through combining the costs to business and the costs to Ofgem the total social costs are calculated. The results are shown in Table 20.

Table 20: Total social costs

Total social costs (2025£m, cumulative 2025-34, discounted)	Option 2	Option 3
Low	54	66
Central	87	97
High	121	128

The vast majority of costs arising from the new load control licence are costs to business. Only energy companies engaging in CLF in the roles of FSPs and/or LCs are affected.

5 Impact on small and micro businesses

As set out in Table 17 Government estimates that 17 small companies are in scope of the new load control licence. Due to exemptions in reporting requirements, it is not trivial to determine the number of micro sized entities. Internal research suggests that up to five companies listed as small could be micro-sized entities.

The estimated costs per individual small company are set out in Table 15 and Table 16. For FSPs ongoing annual costs range from £143,000 to £352,000 for both options. For LCs estimates range from £209,000 to £292,000 in Option 2 and from £290,000 to £339,000 in Option 3.

Two of the cost categories comprising a majority of the costs are management controls and customer protection. As set out above, these are both areas where the 2024 consultation only covered high level policy proposals and did not include details of the proposed licence conditions underpinning company obligations and resultant costs. Little detail was included on Ofgem's approach to administering the licence obligations, which also has an impact on the costs to companies. Ofgem are publishing a consultation on their approach to implementing the licensing regime in parallel to this consultation. We are seeking to validate the cost assumptions through consultation questions 15 and 30.

Nonetheless, the responses, albeit limited, suggest a trend that small companies may face higher costs than medium or large companies. This may likely be because large companies will have implemented many, if not all, of the changes mandated by the licence whereas small companies often have not.

For all categories, in differing degrees of severity, the costs to licensees inversely scale with company size. Large companies could face lower additional costs than small companies. This suggests smaller companies may bear a larger share of the additional costs this policy would require. This consultation provides an opportunity to validate cost assumptions and these trends. The draft licence conditions accompanying this consultation and Ofgem's implementation consultation offer respondents a much higher level of detail to assess the impact of the proposed licence requirements on FTE resource and associated costs. Upon validating the cost assumptions, government will determine whether an approach to mitigating risks to small companies is required.

As set out in the long list discussion above as well as in detail in Table 21 two mitigations have been considered: the tiering of customer protection requirements and the tiering of cyber security requirements.

Tiering of customer protection requirements would mean that FSPs (for both options) below a threshold number of customers would have to comply with more moderate requirements than FSPs above the threshold. Assuming that customer numbers correlate with the number of employees, annual turnover or balance sheet size of an FSP (the criteria for company size), threshold could have been designed to target small companies. However, tiering of customer protection requirements, at this time, was deemed unsuitable due to poor strategic fit. There may be a misallocation of consumers' needs and service standards. Consumers with higher needs may not receive support they require because they are contracted with a lower tier FSP. Further, the creation of more than one level of consumer protection creates a significant risk of consumer confusion and consequently distrust in CLF. There is also the risk that large FSPs avoid obligations through subsidiaries and that consumer protection standards would be eroded over time.

Tiering of cyber security requirements has been explored through the short list appraisal. In Option 2 LCs which control above a certain threshold of electrical load would be subject to tighter cyber security requirements. In Option 3 all LCs follow the same tight cyber security requirements. The cost premium of Option 3 over Option 2 for any one small LC is £47,000 to £81,000 per annum. In total Option 3 creates £7m to £11m additional costs to businesses. Yet the government does not expect significant additional cyber security benefits for this additional cost as small and micro-sized LCs are particularly unlikely to be attacked in the first place. For the electricity grid, it is especially important that large LCs are well protected. Hence, the tiered approach to cyber security, Option 2, is the preferred option for implementation. Load controllers above 300MW will have to meet tier 1 CAF outcomes, while LCs below 300MW will only have to meet tier 2 CAF outcomes. This means a lower cost burden for small LCs. The 300MW threshold was chosen for grid security purposes. Hence, it is possible that some LCs who technically qualify as small companies will be classified as tier 1 load controllers if they control more than 300MW of load.

6 Costs and benefits to households

6.1 Impact on households with Energy Smart Appliances (ESAs)

One of the main intended outcomes of the load control licence is the protection of consumers with domestic energy smart appliances from customer harm and cyber security risks when they engage in load control. CLF and load control can save households with ESAs on their electricity bills. Just through managing charging according to a static time-of-use-tariff EV owners with an average driving pattern and with access to a home charge point can save up to £330 per year.[47] Savings from direct load control should exceed that as they give the load controller more access to potential revenues from flexibility markets. Due to the diversity of households and energy consumption behaviours it has not been possible to quantify or monetise the value of this protection for these households.

It should be noted that currently not all households can engage and benefit from direct load control. ESAs such as EVs and charge points as well as home batteries or heat pumps are still not widely rolled out, even though take up is growing, because of the sizeable up-front investment costs required. Additionally, consumers who do not own the home they live in often lack authority or incentive to install ESAs. A 2019 LCP Delta report for Citizens Advice report assessed the barriers to domestic CLF and named insufficient savings and being a renter as major barriers for CLF engagement besides digital exclusion and a lack of trust/ motivation.[48]

Whilst broadly enabling benefits in the form of risk mitigating for households with ESAs that can engage load control, the licence also has the potential to curtail the load control market and to reduce the attractiveness of load control offers. The additional costs for LCs and FSPs set out in section 4.2.2 need to be recovered. This could take the form of higher costs for consumers. Yet, many licensees do not directly sell services to customers but generate revenues through participation in explicit CLF markets such as NESO's demand flexibility service.[49] Additional licence costs have to be funded through these income streams, which could mean that licensees will have to offer less attractive offers to consumers. In extreme cases it may lead to FSPs/ LCs leave the market which would result in reduced choice for consumers.

6.2 Impact on all households (including households without ESAs)

As set out above, CLF has the potential to reduce GB peak electricity demand which would allow for a more prudent electricity system with more efficient use of generation and network infrastructure. The Electricity Networks Strategic Framework analysis has estimated this benefit to be £40-50bn (cumulative between 2022 and 2050).[50] These savings should result in lower bills for all consumers, including those households that do not own ESAs. It is worth noting that these savings are generated against a theoretical counterfactual of an electricity system without any CLF. As set out above as well, many factors are needed to successfully enable CLF in GB besides the load control licence.

[47] GOV.UK, 'Default energy tariffs for households: call for evidence' (viewed on 8 December 2025)
[48] LCP Delta, 'How accessible are future energy supply business models? A report for Citizens Advice' (viewed on 8 December 2025)
[49] NESO, 'Demand Flexibility Service explained' (viewed on 8 December 2025)
[50] GOV.UK, 'Electricity networks strategic framework: Enabling a secure, net zero energy system' (viewed on 8 December 2025)

Supporting consumer trust for those households that own ESAs and engage in load control through the licence will pay dividends to all consumers.

The second intended outcome of the load control licence is cyber and grid security, which everyone in GB will benefit from including households who do not own ESAs.

7 Business environment

The GB electricity system is the market leader for CLF in Europe.[51] The new load control licence has the potential to support this development but also creates risks to business and investment.

The load control licence is a market enabler because it levels the playing field. All FSPs have to follow the same minimum customer protection standards, and all LCs have to follow the same minimum grid stability and cyber security standards. “Bad actors” cannot undercut serious actors by saving on customer support and protection or cyber security. This reduces the risk of consumer harm and cyber incidents, which enhances the overall reputation of CLF and load control to boost consumer confidence. Consumer confidence is crucial to attract new consumers to engage in CLF and for the overall CLF market to grow.

Standardisation and regulating load control activities, like all regulation, has the potential to hamper innovation. There is a risk that new ways of managing load effectively are implicitly banned through the licence. To mitigate this risk, the licence is introduced in phases, with the set of licence conditions subject to this appraisal only being the first phase and the minimum requirements to ensure customer protection and cyber security.

New regulation often creates a barrier to market entry for new participants. The load control licence is no different. As set out above, the costs of complying with the licence are significantly higher for small businesses as these often have to introduce proportionately larger changes to their organisations than large businesses, who may already be compliant in some respects. These costs could deter businesses or individuals from entering the load control market. To mitigate this risk, the government has tiered cyber security requirements to as set out in more detail in the SaMB assessment (section 5).

8 Other wider impacts

8.1 Impact on rural areas

Average broadband speeds in rural areas tend to be slower than those in urban areas. This is because there is less superfast broadband, and rural premises are typically further away from cabinets with longer line connections which can slow performance. Additionally, rural areas have lower coverage from 4G and 5G coverage. The smart functionality of ESAs and load control require internet connection via broadband or mobile data. Therefore, reduced broadband and network coverage could act as a disincentive for consumers in rural areas to engage in load control or they might experience diminished performance of their ESAs. The disparity in broadband and network across UK regions is being addressed by policies such as the Shared Rural Network programme[52] and the Gigabit project.[53] The uptake and

[51] According to LCP Delta’s 2024 Market Monitor for Demand Flexibility GB has the more elements of the system accessible to CLF than other countries in Europe. LCP Delta, ‘2024 Market Monitor: For Demand Side Flexibility’ (viewed on 8 December 2025)

[52] GOV.UK, ‘Shared Rural Network (SRN) progress update - September 2024’ (viewed on 8 December 2025)

[53] GOV.UK, ‘Project Gigabit’ (viewed on 8 December 2025)

consumer experience of ESAs across regions can be included in the monitoring and evaluation framework for the licence.

9 Risks and assumptions

The key risk to the cost appraisal in the document arises from sample selection bias. The most sizable cost categories in the cost to businesses assessment are management controls, consumer protection and cyber security. The data underpinning the cost assumptions comes from either a small number of consultation responses or a post implementation review. Methodologically, these methods of data collection are classified as non-probability sampling where participants choose to participate in a study. Non-probability sampling is considered likely not representative of the entire population because only a specific type of respondent (e.g., those with strong opinions or specific incentives) will participate. Businesses facing higher costs as a result of the licence are incentivised to respond to warn government of the cost to business impact. Business with little cost impact are not. This would imply upward sample selection bias to be part of the cost assumptions and estimates.

Additionally, there is an incentive for businesses to overinflate their cost estimates to encourage government to scale back requirements to avoid overburdening business. For both reasons, there is a risk that the cost estimates of this document are overinflated. Nonetheless, they can be interpreted as a useful indicative conservative estimate. Though it will suffer from the same methodological weaknesses, several questions have been inserted into the consultation to gather further cost information for the final stage impact assessment.

As set out in Table 6, the cost impacts of general provisions and service exit have not been monetised for a lack of cost data. To improve the evidence base for the final stage impact assessment, questions 12 and 33 have been inserted into the consultation to gather information from the market.

10 Appendix

Long list appraisal

As detailed in section 3.1 Long list appraisal, the government considered the following long list of options to deliver the objectives:

Option 1: Do Nothing - Voluntary, industry led standards
Option 2a) Load Control Licence with tiered consumer protection
Option 2b) Load Control Licence with tiered cyber security
Option 2c) Load Control Licence without tiering
Option 3: Load control licence + a new load control industry code

To assess the suitability of the long list options, the following critical success factors were employed.

1. Strategic fit. Is the option suitable to deliver the objectives of 'Enabling increased uptake of domestic CLF' and 'Preparing our electricity system for increased uptake of domestic CLF'?
   Domestic CLF is a nascent market. Many FSPs currently operate with small profit margins. To grow the domestic CLF market, regulations need to strike the right balance to encourage an expansion of CLF services and ensure integrity of the system whilst avoiding any undue cost burdens for businesses.
2. Value for money. Is the option suitable to deliver the programme objectives at the least cost to business?
3. Affordability Is the option suitable to deliver the programme objectives at the least cost to the tax- or bill payer?
4. Achievability. Is the option deliverable and can be implemented in a timely way to achieve objectives?

Table 21 below sets out the details of the assessment process.

Voluntary standards leave an excessive risk of consumer harm or grid disruption. Hence, Option 1 was excluded due its poor strategic fit. Introducing a new industry code would risk stifling innovation in a nascent market and would be very complex and time consuming to implement. Hence, Option 3 was excluded due to weak strategic fit and poor achievability.

The preferred option is a load control licence (Option 2). As set out in more detail in Table 21 tiering of consumer protection requirements was deemed to undermine the core objective of the licence. Tiering of cyber security requirements (Option 2b) is the governments preferred option because in this option, the requirements are tailored to the cyber security risk an organisation creates to the system.

Table 21: Long list assessment, full details

Long list Options	Strategic fit	Value for money	Affordability	Achievability
Option I: Do Nothing - Voluntary, industry led standards	Existing consumer protection regulation provides general level of protection delivering a base level of confidence. By doing nothing to enshrine further protections against the risks specific to load control, consumers may suffer harm without access to any form of recourse. This could cause damage to consumer trust and uptake. Without cyber security regulations LCs are vulnerable to wider cyber-attacks which could lead to loss of consumer data, loss of smart services and at scale, could lead to impacts on grid stability. Price competition could incentivise FSPs and LCs to cut costs for consumer service and cyber security provisions leading to an erosion of standards across the markets.	No significant cost to businesses as no additional regulations are introduced. The higher risk of large scale cyber attacks and black-outs could result in significant costs to business.	No significant cost to government or bill payers as no additional enforcement or governance activity required. The higher risk of large scale cyber attacks and black-outs could result in significant costs to government.	High achievability as FSPs and LCs could implement the solutions that suit themselves best.
Option IIa) Tiered licence – consumer protection + cyber security	A licence and the associated enforcement through Ofgem would create a very strong incentive for FSPs and LCs to implement effective consumer protection and cyber security measures. However, there may be a misallocation of consumers needs and service standards. Consumers with higher needs may not receive support they require because they are contracted with a lower tier FSP. Creating more than one level of consumer protection creates a significant risk of consumer confusion and consequently distrust in CLF. There is also the risk that large FSPs avoid obligations through subsidiaries and that consumer protection standards would be eroded over time. The risk of a cyber attack on a LC rises the more load they control. Hence, tiering of cyber security requirements is appropriate. There is a slight risk that excessive regulation may hamper innovation and create additional costs for load control consumers.	Application, compliance and reporting would create costs to business that are assumed to be passed down to consumers. The scale of costs would be mitigated for smaller LCs and FSPs through tiering.	Enforcement by Ofgem would create additional costs to consumers. As set out in this document, these would not be very significant against the size of the future load control market.	The implementation of a licensing regime including enforcement is complex and carries the risk of delay to implementation. Practical enforcement of tiered consumer protection standards would be complex for Ofgem as consumer numbers may have to be constantly monitored to ensure the right tiering bracket.
Option IIb) Tiered licence – cyber security	A licence and the associated enforcement through Ofgem would create a very strong incentive for FSPs and LCs to implement effective consumer protection and cyber security measures. Standardisation of minimum consumer protection standards would create stable market conditions. The risk of a cyber attack on a LC rises the more load they control. Hence, tiering of cyber security requirements is appropriate and helps to mitigate the administrative burden higher cyber security standards on smaller players. There is a slight risk that excessive regulation may hamper innovation and create additional costs for load control consumers.	Application, compliance and reporting would create costs to business that would be passed down to consumers. The scale of costs would be mitigated for smaller LCs and FSPs through tiering.	Enforcement by Ofgem would create additional costs to consumers. As set out in this document, these would not be very significant against the size of the future load control market.	The implementation of a licensing regime including enforcement is complex and carries the risk of delay to implementation. Practical enforcement of tiered cyber protection standards would be complex load control levels may have to be monitored to ensure the right tiering bracket.

Long list Options	Strategic fit	Value for money	Affordability	Achievability
Option IIc: untiered licence	A licence and the associated enforcement through Ofgem would create a very strong incentive for FSPs and LCs to implement effective consumer protection and cyber security measures. Standardisation of minimum standards would create stable market conditions. A totally untiered approach to licensing risks that excessive regulation may hamper innovation, create additional costs for load control consumers and inhibit the growth of the domestic and small non-domestic CLF market.	Application, compliance and reporting would create costs to business that would be passed down to consumers.	Enforcement by Ofgem would create additional costs to consumers. As set out in this document, these would not be very significant against the size of the future load control market.	The implementation of a licensing regime including enforcement is complex and carries the risk of delay to implementation.
Option III: Load control licence + a new load control industry code	An industry code would be able to prescribe very detailed consumer protection and cyber security requirements. This greater level of detail creates a significant risk of stifling innovation given the still nascent CLF market.	Code development and consultation engagement as well as reorganisation for compliance would create significant costs to business.	Given the greater level of complexity of a code, enforcement action for Ofgem may be more costly, albeit not dramatically.	Creating and updating industry codes is a long process and carries the risk of delay to implementation. The creation of another code manager adds additional complexity into the electricity system governance structure.

Break-even analysis of cyber security benefits

The central idea of break-even analysis is to find out how much benefit is needed to justify the costs. Then one can judge whether this benefit seems realistic. Applied to cyber security benefits of the load control licence this translates into the following question: *How many households, and for how long, would need to be affected by a disruption for the cost of preventing it through the cyber requirements in the licence to be justified?*

In a first step the cyber security related costs of the licence need to be isolated. The total, cumulative discounted costs are shown below.

Table 22: Total discounted cyber security costs

Total cyber security costs £2025m, discounted	Option 2	Option 3
Low	14	26
Central	19	28
High	24	30

Grid disruption and blackouts lead to real economic damage as Table 3 shows. The benefit of cyber and grid stability requirements is realised through the reduction in grid disruption and blackouts caused by cyber-attacks through load controllers. To value the damage of grid disruption government used the concept of "Value of lost load" (VoLL). VoLL is used to inform the upper limit of acceptable costs to stabilise the electricity system. If an action costs more than VoLL, it is assumed that consumers rather incur a power cut than incur the costs of preventing it. In this analysis a VoLL estimate of 23,730 £2025/MWh is used.[54] With the help of VoLL the load loss duration equivalent to licence cyber costs can be calculated (Break-even load loss).

The results in Table 4 show total discounted cyber costs over the ten-year appraisal period are equivalent to the economic damage from 602MWh to 1000 MWh for Option 2 and 1085MWh to 1276MWh for Option 3.

Table 23: Cyber Benefits - Break-even load loss

Break even load loss (MWh)	Option 2	Option 3
Low	602	1085
Central	791	1181
High	1000	1276

Based on the average annual household consumption in the UK,[55] this is equivalent to 0.25% to 0.41% of households losing electricity for one day in Option 2 (0.45% to 0.53% in Option 3) in one instance in the next 10 years. This shows that a one day interruption of supply for less than 1% of households is worth the costs of the cyber protection requirements.[56] If one believes that CLF cyber-attacks through load controllers could lead

[54] London Economics, 'The Value of Lost Load (VoLL) for Electricity in Great Britain, Final report for OFGEM and DECC' (viewed on 8 December 2025)

[55] The average household electricity in the UK in 2024 was 3,090 MWh. GOV.UK, 'Average annual domestic electricity bills by various consumption levels (QEP 2.2.5)' (viewed on 8 December 2025)

[56] One can extrapolate this to conclude that the damage of even a short national blackout would vastly exceed the cyber costs of the licence for both options.

to more load loss than that in the next 10 years, cyber licence conditions deliver value for money.

Table 24: Cyber benefits – Break-even household supply interruption

	Days of interrupted HH supply (thousands)		Share of UK households with 1 day of interrupted supply	
	Option 2	Option 3	Option 2	Option 3
Low	71	128	0.25%	0.45%
Central	93	139	0.33%	0.49%
High	118	151	0.41%	0.53%

Costs per licensee – detailed cost summary

Table 25: Detailed summery of all cost per licensee assumptions, 2025£ thousands

Company Size	Small			Medium			Large		
Sensitivity	L	C	H	L	C	H	L	C	H
	Set up (Year 1)								
Code compliance	4	4	4	4	4	4	4	4	4
Management controls	98	98	98	49	49	49	12	12	12
Data provision	7	16	24	7	16	24	7	16	24
Grid Stability	7	7	7	7	7	7	4	4	4
Cyber security	159	210	267	159	210	267	288	315	342
Customer protection	34	131	227	34	131	227	0	88	176
Service Exit	0	0	0	0	0	0	0	0	0
	Ongoing (Year 2 and following)								
Code compliance	4	4	4	4	4	4	4	4	4
Management controls	98	98	98	49	49	49	12	12	12
Data provision	7	16	24	7	16	24	7	16	24
Grid Stability	0	0	0	0	0	0	0	0	0
Cyber security	100	132	167	100	132	167	182	198	214
Customer protection	34	131	227	34	131	227	0	88	176
Service Exit	0	0	0	0	0	0	0	0	0

It is worth noting that the cyber security costs for large licensees are counted as zero in the total cost to business and the total social costs as cyber requirements for large load controllers are enforced through trough the NIS regime.