Department for
Business, Energy
& Industrial Strategy

Delivering a smart and secure electricity system

Consultation on interoperability and cyber security of energy smart appliances and remote load control

Closing date: 28th September 2022

July 2022

Any enquiries regarding this publication should be sent to us at:
SSESconsultation@beis.gov.uk

General information

Why we are consulting

A smart and flexible electricity system is critical to decarbonise our economy, help manage electricity demand and reduce consumer bills. Energy smart appliances like electric vehicle charge points and smart heat pumps, as well as organisations who provide services to consumers to manage their electricity usage, will play an important role in this future energy system by providing “flexible demand” services.

The Government consulted on regulating energy smart appliances in 2018, and electric vehicle smart charging in 2019. In the Smart Systems and Flexibility Plan 2021, we committed to consult on regulating flexibility service providers and other organisations controlling electrical load. This consultation follows on from this publication, setting out a range of proposals that will impact appliances and organisations with a role in controlling electricity usage.

Consultation details

Issued: July 6th 2022

Respond by: September 28th 2022

Enquiries to: SSESconsultation@beis.gov.uk

Consultation reference: Delivering a smart and secure electricity system - Consultation on interoperability and cyber security of energy smart appliances and remote load control

Audiences: This consultation will be of interest to energy consumers, companies in the energy sector, heat pump and wider energy smart appliance manufacturers, innovators, technology companies (including charge point operators), third party intermediaries in energy and/or other sectors and consumer and environmental groups.

Territorial extent: Great Britain.

How to respond

Responses are encouraged to be provided via the response word document template that can be found on the GOV.UK consultation page: www.gov.uk/government/consultations/delivering-a-smart-and-secure-electricity-system-the-interoperability-and-cyber-security-of-energy-smart-appliances-and-remote-load-control.

This response word template can be sent via email to SSESconsultation@beis.gov.uk or our postal address.

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

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

Email response form to: SSESconsultation@beis.gov.uk

or

Post response form to:

SSES team (NZEN)
Department for Business, Energy and Industrial Strategy
3rd Floor
1 Victoria Street
London
SW1H 0ET

Confidentiality and data protection

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

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

We will process your personal data in accordance with all applicable data protection laws. See privacy policy.

We will summarise all responses and publish this summary on GOV.UK. The summary will include a list of names or organisations that responded, but not people's personal names, addresses or other contact details.

Quality assurance

This consultation has been carried out in accordance with the Government's consultation principles. If you have any complaints about the way this consultation has been conducted, please email: beis.bru@beis.gov.uk.

Executive Summary

As our economy and energy system undergo a transformation to net zero carbon emissions and to energy independence, new products and services will increasingly come to market to aid our transition to a smart and flexible energy system. Energy smart appliances (ESAs) and services that manage energy usage for consumers will be part of this new wave of consumer offerings. These appliances and services will provide an essential source of flexibility through "demand-side response" (DSR), which allows consumers to use electricity when they need it, at a lower cost, whilst enabling electricity to be more efficiently distributed on our electricity system. Through DSR, small changes in energy consumption by many thousands or millions of consumers and devices can collectively help flatten overall peaks in electricity demand. This reduces the need for more carbon intensive generation, helps accommodate more low-carbon generation, and reduces the overall costs of managing the electricity network, lowering bills for everyone. In addition, it empowers consumers, giving them the opportunity to minimise their bills and to earn revenue in exchange for the value they provide to the electricity system.

Some of these services are already being provided today on a small scale for domestic consumers. For example, electric vehicle (EV) owners can get discounts, rewards or cash-back by charging their car during periods of the day when electricity demand is typically low. With an increased use of these services, alongside use of interconnectors and storage, the costs of managing our electricity system could be reduced by £10 billion a year by 2050.

However, there are currently barriers to the growth of this sector. Not all tariffs and services are available for all devices, and there are limited consumer protections to build confidence in the market. In addition, greater use of ESAs and other associated services could pose risks to the energy system, such as creating new routes for cyber security attack.

To ensure we achieve a smart, secure, and flexible electricity system, action is needed to enable the market for DSR to grow, and to prepare our electricity system for its potential mass uptake. Ensuring we maintain and empower consumers' choice to use DSR services will be crucial part of building confidence in the market. As such, our proposals will help ensure consumers who choose to use such services, have a wide range of options, and receive fair contractual arrangements. The Government has previously set out proposals for regulating energy smart appliances and required private EV charge points to have smart functionality. This consultation builds off these proposals, setting out actions to ensure consumers and the electricity system are protected, and to develop a competitive market for energy smart appliances and DSR. These proposals aim to provide a triple win for consumers, industry, and the energy system: lowering consumer bills, enabling the growth of innovative companies, and improving the security of Britain's electricity system.

Our proposals are focussed on three key areas:

- **Creating the right technical frameworks to unlock the potential of flexibility for domestic and small non-domestic energy consumers:** standardising how tariff

information is shared and building on existing standards to ensure that energy smart appliances can access different tariffs and flexibility services.

- **Improving the security of the electricity system:** developing new cyber security and grid stability requirements to ensure that the increasing number of organisations who can remotely control substantial amounts of electrical load, do so in a way which protects the electricity system and effectively manages potential cyber security and grid stability risks.
- **Giving consumers confidence to engage with a smart energy system:** introducing measures affecting both energy smart appliances and DSR service providers to establish minimum standards that help build confidence in this emerging but crucial market, and to ensure a level playing field for organisations providing services to consumers who choose to adopt them.

To deliver on these objectives, our consultation covers several areas, and respondents may want to respond to all or some of these depending on their interests. We propose:

- To require all organisations controlling large electrical loads (greater than 300MW) to comply with the provisions of the Network and Information Systems Regulations, and to be assured by the Cyber Assessment Framework. This is an important measure to improve security of the energy system as a whole and to mitigate the risks of potentially highly disruptive cyber-attacks. **(Chapter 2)**
- To require energy suppliers to make time-of-use tariff data openly available in a common format, accessible over the internet. This will make it easier to ensure that energy smart appliances are compatible with different tariffs, enabling greater uptake of smarter and more dynamic time-of-use tariffs. **(Chapters 3-5)**
- To ensure that larger domestic-scale ESAs, including private EV charge points, batteries, heat pumps, storage heaters and heat batteries are interoperable with DSR service providers, using the industry-led standard, PAS 1878, as the basis for future requirements, and to seek views on the appropriate regulatory framework to deliver this. This will enable consumers and innovative companies to unlock more advanced forms of flexibility at scale and give consumers greater choice by ensuring that smart appliances are compatible with all flexibility services in future. **(Chapters 3-5)**
- To require larger domestic-scale ESAs to meet minimum cyber security and grid stability requirements, like those already in place for EV charge points. In addition, we will work with the National Cyber Security Centre (NCSC) to consider what further interventions may be required to manage cyber security risks posed by the growth in deployment of ESAs. Together with the other requirements outlined in this consultation, this will ensure a holistic framework is established to mitigate cyber security risks that ESAs could otherwise pose to the energy system and to consumers. **(Chapters 3-5)**
- To establish comprehensive governance arrangements between Government, regulators, and industry to support implementation of the proposals for ESAs. This will be important both to develop the technical detail necessary to realise the proposals outlined in this consultation, and to put in place mechanisms for longer-term

maintenance and updating of standards that underpin the smart energy system. **(Chapter 5)**

- To require electric heating appliances with the greatest flexibility potential, namely heat pumps, storage heaters, and heat batteries, to have 'smart' functionality. This will help build in the benefits of flexibility in parallel to scaling up deployment of electric heating – helping ensure we can effectively integrate the expected rapid increase of heat pumps and other electric heating appliances into the energy system in the most cost-effective and beneficial way for consumers. It will ensure that all consumers are more easily able to use their devices to access smart tariffs and services if they choose to do so. **(Chapter 6)**
- To establish a proportionate and flexible licensing framework for organisations providing demand side response to domestic and small non-domestic consumers. This will ensure that organisations who operate energy smart appliances do so responsibly and in a way which enables markets to grow, while also safeguarding consumer confidence. **(Chapter 7)**

Government is seeking enabling powers via the Energy Security Bill, introduced on 6 July, and this consultation focuses on how those powers would be implemented. We recognise that this is a broad and ambitious package of proposals, aiming to establish a comprehensive and dynamic framework that can stand the test of time. We propose that implementation would be phased to give time for Government and industry to work together to address the most significant and near-term opportunities and risks first. To ensure we build in industry and consumer views from the outset, this consultation seeks views on our overarching direction of travel. Further consultations will be carried out on the technical detail ahead of implementation. While the Bill is accompanied by an economic impact assessment, future regulations will also be accompanied by further economic impact assessments, and spending measures will be subject to value for money assessment.

Contents

General information 3
Executive Summary 5
1. Introduction 9
2. Cyber security proposals for protecting the energy system 17
3. Energy smart appliances: Outcomes 24
4. Energy smart appliances: Technical frameworks 30
5. Energy smart appliances: Delivery frameworks 44
6. Smart Electric Heating 52
7. Regulation of organisations 57
8. Next steps 64
Consultation questions 65
Appendix 1: Summary of impacts 68
Appendix 2: ESA System Overview 69
Appendix 3: Glossary 71

1. Introduction

To decarbonise the power system by 2035, support energy independence and achieve net zero at the least cost by 2050, we will need to transition to a smart and flexible electricity system. The British Energy Security Strategy, published earlier this year, highlights that increased flexibility could help enable the transition away from fossil fuels and reduce electricity system costs, by better managing how and when we use energy[1]. These cost reductions could be worth up to £10 billion per year by 2050[2]. Unlocking these benefits will catalyse our energy transition, lower consumer bills, and help create new commercial opportunities and markets for innovative UK businesses to thrive in.

Demand side response (DSR) – the process of changing when electricity is used or produced by consumers in response to needs of the electricity system – will play a vital role in such flexibility. DSR will help flatten peaks in demand and best utilise low-carbon generation, reducing the costs of managing our net-zero transition. Today, industrial, and commercial consumers are providing around 1GW of DSR to the system[3], but participation from domestic and smaller non-domestic consumers remains low and at an early stage of adoption.

In addition to lowering overall electricity system costs, DSR can help individual consumers lower their own bills through use of “smart” tariffs and other consumer propositions. DSR will also play a role in reducing carbon emissions, through shifting consumption away from times when we are dependent on more carbon-intensive generation, to times when low-carbon energy is more abundant. DSR is a core aspect of Government's strategy to decarbonise energy, as part of the transition to a smart and flexible energy system.

Appliances like electric vehicle charge points and heat pumps have high potential to provide flexibility through DSR. While they will increase demand for electricity, these appliances and others can deliver DSR by changing when electricity is used or produced, to minimise their impact on the energy system. With increased deployment of such appliances, new business models and services will emerge whereby companies remotely manage consumers’ energy smart appliances according to their preferences, to reduce impact on the energy system and subsequently reduce consumer bills. In addition, appliances will be able to optimise energy usage, while also ensuring consumers needs are met. For example, a smart electric vehicle charge point can be programmed to ensure that a consumer’s car is charged when they need it, but it can optimise when the car charges to minimise the energy system impact. This will allow DSR to be delivered ‘behind the scenes’ for consumers, ensuring they still get the same or better service but at lower costs and while retaining choice and control.

[1] https://www.gov.uk/Government/publications/british-energy-security-strategy/british-energy-security-strategy
[2] BEIS (2021), Smart systems and flexibility plan 2021: Appendix I – Electricity system flexibility modelling, p. 5, https://www.gov.uk/Government/publications/transitioning-to-a-net-zero-energy-system-smart-systems-and-flexibility-plan-2021
[3] National Grid (2021), Future Energy Scenarios Data Workbook, Sheet FL.9 https://www.nationalgrideso.com/document/199971/download

We are seeing some of these services coming to market now. For example, EV owners can subscribe to services where they get discounts, rewards or cash-back for letting a third party dynamically control when their car is charged. Some energy suppliers are offering sophisticated time-of-use tariffs that change the price of energy depending on when it is used. Whilst these services are not being offered on a large scale now, the scale of uptake in DSR and ESAs by domestic and small non-domestic consumers has the potential to increase significantly in the future.

However, there are currently barriers to the growth of this sector. Not all tariffs and services are available for all devices, and there are limited consumer protections to build confidence in the market. To ensure we are prepared for the future, the Government is proposing to implement measures to ensure domestic consumers who choose to use DSR services, are able to get the most benefits from doing so, irrespective of the kind of smart appliance and service they choose. These will also help address the current barriers and market failures that prevent more UK businesses from maximising the potential of DSR for their own growth and for the wider economy.

In addition, this consultation includes proposals aiming to ensure that the electricity system is prepared for the mass uptake of ESAs and DSR, through mitigating risks to cyber security and grid stability. Improving resilience to cyber-attack of our critical national infrastructure is a core pillar of the National Cyber Strategy[4]. The number of smart connected appliances is already increasing rapidly[5] and more connected appliances capable of DSR increases the potential for cyber-attack, which could lead to consumer detriment, or even energy system disruption.

Within this consultation, we set out a series of proposals to enable energy smart appliances to work with different DSR service providers and time-of-use tariffs, and to mitigate the consumer protection, cyber security, data privacy, and grid stability risks associated with increased demand side response. These proposals aim to enable the scale-up of competitive markets for DSR and energy smart appliances, by ensuring consumers have confidence in these services, and that the electricity system can accommodate their uptake. The proposals are intended to ensure that more consumers are able to access the benefits of a smart energy system, and can have greater confidence to choose to take up smart tariffs and services.

Policy context

This consultation takes place against a backdrop of wider reform aimed at enabling the growth of new business models that allow consumers to use their energy smart appliances in a smart and flexible way. A series of policy proposals have been announced in recent years that will

[4] Cabinet Office (2022) National Cyber Strategy 2022, https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022

[5] The average UK household is estimated to have had over nine smart appliances in 2020, and forecasts expect up to 50 billion connected appliances worldwide by 2030. (Government response to the call for views on consumer connected product cyber security legislation)

aim to enhance the benefits and mitigate the risks that these business models and appliances could create.

The Government's Secure by Design proposals aim to help ensure consumer's "smart" appliances have security built in from the start[6]. The Government also called for evidence in 2021 on the risk that "load controllers" may pose to the energy system[7]. This year the Government has published a consultation on how to improve the UK's cyber resilience for its most critical sectors via amending the Network and Information Systems (NIS) Regulations[8]. In addition, following legislation, from the end of June 2022 all EV charge points sold in Great Britain are required to meet minimum cyber security requirements and have smart functionality[9]. In future, Ofgem's implementation of market-wide half-hourly settlement in the mid-2020s will put additional incentives on energy suppliers and other parties to develop more 'smart' tariffs and innovations that help encourage DSR, making greater use of functionalities provided by smart meters.

Building on these wider reforms, this consultation sets out the overarching regulatory framework for technologies and services that will enable flexibility on our electricity system. Within it, we set out proposals for minimum standards to apply to energy smart appliances, including EV charge points and heat pumps, as well as how a proportionate licencing scheme, alongside use of the NIS Regulations[10], can help embed good practice across organisations and improve consumer and energy system protections. Following previous consultations and calls for evidence, Government is seeking enabling powers via the Energy Security Bill, which was introduced on 6 July, and this consultation focuses on the implementation of those powers, to enable regulation of energy smart appliances and organisations that control electrical load.

Internationally, there are also increasing efforts by governments and industry to transition to smarter and more flexible energy systems. For instance, international standards organisations have developed a range of standards relating to smart grids and EV charging. The European Union has also announced plans to develop a code of conduct for energy smart appliance manufacturers.[11] The UK is a global leader in energy system digitalisation and the proposals in this consultation will help to ensure that remains the case. We will also continue to look internationally to share and learn from best practice and where appropriate seek alignment, while protecting the interests and needs of our own consumers and energy system.

[6] https://www.gov.uk/Government/collections/secure-by-design
[7] Third-party intermediaries in the retail energy market: call for evidence
[8] Proposal for legislation to improve the UK's cyber resilience Proposal for legislation to improve the UK's cyber resilience
[9] https://www.gov.uk/Government/consultations/electric-vehicle-smart-charging
[10] https://www.legislation.gov.uk/uksi/2018/506/made
[11] https://ses.jrc.ec.europa.eu/development-of-policy-proposals-for-energy-smart-appliances

Scope and summary of consultation proposals

The below sections discuss the types of appliances and organisations impacted by the above proposals in more detail. A summary of our proposals' impacts can be found in Appendix 1.

Energy smart appliance requirements

Energy smart appliances (ESAs) are electrical consumer devices that are communications-enabled and capable of responding automatically to incentive signals (such as price) and/or other more direct control signals (such as specific instruction to operate at a given power at a certain time of day), by shifting or modulating their electricity consumption and/or production. Appliances with this functionality include EV charge points, batteries, heat pumps, heat batteries, storage heaters, air conditioning/ventilation systems, wet/cold appliances, building energy management systems, smart EV charging cables and solar panels with ‘smart’ storage systems, amongst others.

Different types of ESAs present different risks and opportunities to consumers and the energy system. As such, the proposals in this consultation do not apply uniformly to all ESAs. Our proposals are primarily focused on unlocking flexibility from domestic-scale ESAs with the highest potential for the energy system and consumers. This includes private EV charge points, electric heating appliances (including heat pumps, heat batteries and storage heaters) and batteries.

However, consumers using other ESAs (such as white goods) could still stand to benefit from some of the proposals, through voluntary use of time-of-use tariff data and common standards for interoperability. They may also be included in scope of regulation further into the future, as consumer uptake grows, and markets mature.

A breakdown of several types of ESAs and the impact of our proposals can be found below:

Table 1: Impact of policy proposals in relation to types of Energy Smart Appliance (ESA)

Type of Energy Smart Appliance (ESA)	Proposal
Heat pumps, heat batteries, storage heaters	• To require new appliances to have ‘smart’ functionality. • To meet minimum cyber security and grid stability requirements, similar to those already in place for EV charge points. • To be interoperable with DSR service providers, and to meet further requirements for cyber security, grid stability and data privacy.
Batteries	• To meet minimum cyber security and grid stability requirements, similar to those already in place for EV charge points. • To be interoperable with DSR service providers, and to meet further requirements for cyber security, grid stability and data privacy.

Private (domestic and workplace) EV charge points	• To be interoperable with DSR service providers, and to meet further requirements for cyber security, grid stability and data privacy – in addition to the 2021 Electric Vehicles (Smart Charge Points) Regulations already in place.
Other ESAs, such as white goods and other heating appliances	• Further consideration will be given to the regulatory requirements needed in the future, including the role of a labelling scheme to promote consumer uptake and the adoption of ESA standards.

Organisation requirements

'Load control' is the remote control or configuration of electricity consumption, production, or storage of electricity. This includes sending commands to control the load of an appliance directly or configuring it so that it responds to another signal in the future (such as time or price). The entities who carry out load control are referred to in this consultation as 'load controllers'. Load control can be for different purposes, including DSR and non-DSR (such as a consumer remotely controlling their heating system via an app to turn on before they get home). Load control is a broad concept, capturing a wide group of existing organisations who have different roles in the smart energy system. Several types of load controller will present different benefits and risks to consumers and the energy system, and the proposals in this consultation do not apply to all load controllers and activities uniformly. Examples of load controlling organisations include:

- **DSR Service Providers:** Organisations who remotely control or configure the electricity consumption or production (or contract with consumers for these purposes), typically to benefit organisations responsible for supply, balancing, transmission, or distribution of energy (also known as 'Aggregators' or 'Flexibility Service Providers'). In practice, some energy suppliers are already DSRSPs (Demand Side Response Service Provider) today or may intend to be DSRSPs in the future.

- **Home/Building Energy Management Service Providers:** Organisations who remotely control or configure the energy usage or production of appliances, in response to the energy usage, production or storage of other ESAs within the same premises. This is typically to deliver an outcome (such as EV charge level, temperature etc) optimised against parameters (such as cost) for multiple ESAs.

- **Energy Smart Appliance Operators:** Organisations who provide the systems and connectivity to enable remote control or configuration of ESAs by consumers. In the context of EV charge points, these organisations are often referred to as 'charge point operators'. In today's market, this is typically via a remote, cloud-based operating system. Other solutions, such as physical ESA manufacturer-specific hubs in the home, can provide equivalent functionality.

- **Public Charge Point Operators:** Organisations who provide the public with the capability to charge EVs through charge points that are accessible to the general public.

Our consultation proposes that all organisations which remotely control large amounts of load (greater than 300MW) should be brought into scope of the Network and Information Systems Regulations. In addition, building off previous Government publications[12], we propose regulating organisations involved in providing DSR for domestic and small non-domestic consumers, through a proportionate and flexible licensing framework. This reflects the potential barriers to promoting uptake of DSR from these consumers, and the greater consumer risks for domestic consumers. It also reflects the greater maturity of DSR from larger businesses, and the market-led solutions to enable DSR uptake in these more established markets.

We recognise our proposals do not cover all aspects of load control. For instance, domestic scale appliances not used for DSR, such as home assistants, which may be used to remotely control other smart appliances in the home. Our proposals also only consider industrial and commercial scale DSR insofar as it relates to cyber security. This is because we have not identified evidence to suggest further intervention is needed in these areas. However, we welcome views on this approach.

Legislative approach

Following our 2018 consultation on setting standards for energy smart appliances[13] and 2019 call for evidence on the long-term approach to electric vehicle smart charging[14], and in line with our commitment in the Smart Systems and Flexibility Plan 2021, Government is seeking enabling powers through the Energy Security Bill to: (i) regulate ESAs, (ii) set minimum standards for smart functionality for certain ESAs, (iii) license activity relating to load control. The Bill, introduced to Parliament on 6 July 2022, will enable the following:

- **Powers to set requirements for energy smart appliances:** The Bill will provide Government with the power to introduce regulations for energy smart appliances (such as smart EV chargepoints and smart heat pumps) so that devices meet minimum technical requirements for cyber security, interoperability, data privacy and grid stability. This power will also allow Government to mandate that electric heating appliances must have smart functionality, prohibiting the sale of non-smart heating appliances in Great Britain. The same power will also be used for private EV chargepoints. Although there are existing powers which allow government to make regulations for smart EV chargepoints, this new additional power is needed to ensure that a cohesive approach is taken to regulating all energy smart appliances, given the degree of similarity across this cohort of devices.

- **Powers to make activities related to load control licensable:** The Bill will provide powers to enable government to regulate organisations who are involved in remotely controlling these smart devices, through making activities related to the provision of load

[12] In the Government Response to the 2019 Consultation on Electric Vehicle Smart Charging, we committed to future policy development on a wider range of organisations performing a "load controlling" role
[13] https://www.gov.uk/Government/consultations/proposals-regarding-setting-standards-for-smart-appliances
[14] OZEV (2019) Consultation on electric vehicle smart charging https://www.gov.uk/government/consultations/electric-vehicle-smart-charging

control into licensable activities. This will ensure they operate in a way which is beneficial for consumers and the grid, for example meeting requirements for consumer protection and cyber security.

The Bill itself will not create any immediate new requirements but will provide the powers needed to develop secondary legislation. This consultation focuses on implementation of the above powers by secondary legislation, subject to approval by Parliament.

Interaction with existing regulation for electric vehicle charge points

Using the powers in the Automated and Electric Vehicles Act 2018[15], Government has already acted via the Electric Vehicle (Smart Charge Points) Regulations 2021 to require private EV charge points to have smart functionality and meet minimum appliance-level standards relating to cyber security and grid stability. As set out in the 2019 consultation on electric vehicle smart charging and subsequent Government response, this is just the first phase of regulation needed to ensure charge points are secure and consumers are protected. The proposals in this consultation set out the next phase of work for EV charge points and other ESAs. The powers Government is seeking via the Energy Security Bill will extend to private EV charge points, enabling a cohesive legislative approach for all ESAs under a single set of powers. Aligning the primary powers will enable a consistent regulatory regime for all ESAs, helping create a level regulatory playing field, benefiting both the market and consumers. This will enable a single, technology-neutral approach that can evolve over time.

Implementation

The proposals within the consultation have different levels of complexity, benefit, and cost to deliver. Government therefore anticipates implementing these proposals over a period of several years. Our intent is to prioritise interventions that mitigate the most pressing risks or unlock the most significant benefits, such as interoperability of time-of-use tariffs and minimum cyber security requirements for ESAs. As such, we are taking a phased approach to implementation, with some measures potentially applying from 2024, subject to the outcome of this consultation and parliamentary time. However, pace of implementation will depend on outstanding policy decisions and availability of parliamentary time, making exact implementation dates uncertain at this stage. The governance arrangements proposed in Chapter 5 intend to provide a mechanism for plans to be developed with impacted stakeholders and seek views on what is required to move from policy proposals to full implementation. The expected phasing is summarised in Table 2 below. Implementation will be supported by further consultation on future detail, where appropriate. Whilst the Energy Security Bill is accompanied by an impact assessment, secondary legislation related to this consultation's proposals will also need to be subject to full impact assessments to ensure that the costs of our proposals are proportionate to the benefits. In addition to this consultation, we

[15] https://www.legislation.gov.uk/ukpga/2018/18/contents/enacted

have published an analytical annex which sets out a series of questions to help strengthen the analysis that will inform future consultations and their impact assessments.

Table 2: Proposed phased approach to implementing policy proposals

Phase	Proposal
Short-Term *(by the mid-2020s)*	• To require energy suppliers to make time-of-use tariff data openly available in a common format, accessible over the internet. • To require domestic-scale ESAs, including heat pumps, storage heaters, heat batteries and batteries, to meet minimum cyber security and grid stability requirements, similar to those recently established for private electric vehicle (EV) charge points.
Medium-Term *(mid-2020s)*	• To require heating appliances with the greatest flexibility potential, namely heat pumps, storage heaters, and heat batteries, to have 'smart' functionality. • To establish a proportionate and flexible licensing framework for organisations providing DSR to domestic and small-non-domestic consumers, regulated by Ofgem. • To require larger load controllers to comply with the provisions of the NIS Regulations, and to be assured by the Cyber Assessment Framework.
Long-Term *(mid-late 2020s)*	• To require larger domestic-scale energy smart appliances, such as EV charge points, batteries, and heat pumps, to be fully interoperable with DSR service providers, and to meet further requirements for cyber security, grid stability and data privacy.

1. **What are your views on the over-arching timings of implementation of these proposals, including the proposed approach to phasing?**

2. Cyber security proposals for protecting the energy system

The purpose of this chapter is to establish the cyber security approach Government intends to promote in future policy for load controllers.

Strategic Context

The cyber threat to the UK continues to grow and evolve. According to the Cyber Security Breaches Survey 2022[16], two in five businesses (39%) report having experienced cyber security breaches or attacks in the last 12 months. Among the businesses that identify breaches or attacks, almost a third (31%) are experiencing these issues at least once a week. However, only just over half of organisations (54%) have taken any action to help identify cyber security risks in the last twelve months.

Cyber-attacks against the energy sector have the potential to pose a risk to national security, the economy, and could impact on the essential energy services that we all rely on every day. The energy sector is undergoing a significant transformation, becoming increasingly digitised and decentralised. New cyber security risks will emerge as the energy system becomes more connected and driven by data and technology. It is essential that the UK's smart energy system remains a safe, resilient system.

The National Cyber Strategy 2022[17] is our plan to ensure that the UK remains confident, capable, and resilient in a fast-moving digital world, and that we continue to adapt, innovate, and invest to protect and promote our interests in cyberspace.

Significant progress has been made in improving cyber resilience across the economy. However, with many organisations still reporting high numbers of cyber security breaches or attacks, serious gaps remain. To address this, the National Cyber Strategy 2022 commits to strengthen the coverage, powers, and agility of the legislative framework to adapt to changing security risks, threats, and technologies. Proposals in this consultation strongly support the resilience pillar of the strategy. This pillar aims to secure systems to:

- Understand cyber risks;
- Prevent and resist cyber-attacks; and
- Prepare, respond, and recover from cyber-attack.

The Network and Information Systems (NIS) Regulations[18] establish legal requirements on specific critical sectors, including the energy sector, to boost the overall level of security of network and information systems that are critical for the provision of essential services in that

[16] DCMS (2022) Cyber Security Breaches Survey 2022, https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2022/cyber-security-breaches-survey-2022
[17] Cabinet Office (2022) National Cyber Security Strategy 2022, https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022
[18] The Network and Information Systems Regulations 2018, https://www.legislation.gov.uk/uksi/2018/506/made

sector. In January 2022, Government published a consultation[19] with proposals to amend the NIS Regulations to further improve the UK's cyber resilience across critical sectors. One such proposal is to introduce delegated powers to extend the scope of the regulations to additional subsectors and essential services. The consultation mentioned energy management service providers and DSRSPs, such as EV charge point operators, as examples for potential scope extension in the energy sector. Subject to the approval of Parliament, and further consultation, this consultation lays out proposals on how we plan to use these delegated powers to amend the NIS Regulations, and dynamically manage risks associated with the evolving threat landscape and the energy systems transformation.

Cyber Security: The future of the electricity sector and load controllers

As demands for flexibility increase from both the electricity network and from consumers, it is projected that the amount of electrical load controlled by organisations providing DSR will also increase substantially. Beyond providing DSR services, remote load control as a function will become a growing part of other digital business models too, including EV charge point networks. As our energy system becomes more digitalised and interconnected, this means that these different technologies and service providers could introduce new vulnerabilities that could have a system-wide impact.

As load controlling organisations ('load controllers') provide essential services to a more dynamic energy system, the associated increase in digitalisation and remote energy management will also bring new cyber security-related risks to the operation of the electricity sector. Recent high-profile cyber-attacks, such as the December 2020 SolarWinds supply chain compromise[20], the May 2021 ransomware attack on the United States Colonial Pipeline[21], and the July 2021 attack on the managed service provider Kaseya[22] demonstrate how malicious actors can compromise national infrastructure by exploiting companies and products providing essential services, and hence can disrupt activities in the wider economy and society.

There are currently little or no legislative cyber security requirements on load controllers as a whole, and the industry is largely self-regulating via measures such as industry-led codes. However, the National Cyber Security Centre (NCSC) has assessed that voluntary, industry-led codes are unlikely to drive the level of adequate, consistent cyber security resilience necessary for managing the relative risk of cyber-attack in the long-term.

Based on cross sector analysis of market driven cyber security[23], Government has reason to believe that the market alone is not an adequate driver of appropriate and proportionate cyber security. More broadly, the 2019 Cyber Security Incentives and Regulation Call for

[19] DCMS (2022) Proposals for legislation to improve the UK's cyber resilience (2022) https://www.gov.uk/government/consultations/proposal-for-legislation-to-improve-the-uks-cyber-resilience/proposal-for-legislation-to-improve-the-uks-cyber-resilience
[20] https://www.ncsc.gov.uk/report/weekly-threat-report-18th-december-2020
[21] https://www.ncsc.gov.uk/report/weekly-threat-report-14th-may-2021
[22] https://www.ncsc.gov.uk/report/weekly-threat-report-9th-july-2021
[23] DCMS (2022) Cyber Security incentives and regulation review, https://www.gov.uk/government/publications/2022-cyber-security-incentives-and-regulation-review/2022-cyber-security-incentives-and-regulation-review

Evidence[24] found that 71% of respondents agreed that a lack of strong commercial rationale was a barrier for effective cyber risk management. The 2022 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. Organisations the NCSC has engaged with have also highlighted a need for improved assurance to drive greater efficiency and improved consistency in standards and approach. Thus, it is Government's view that intervention is necessary to manage cyber security risks appropriately and proportionately, especially in critical sectors such as energy.

Proposals

It is Government's view that in a smarter, more flexible, and decentralised energy system, load controllers will provide essential services and flexibility in remotely controlling large amounts of electrical load. This will become essential to our critical national infrastructure (CNI) and consumers. Without an appropriate level of cyber security, load controllers will become a point of vulnerability to the broader energy system, as well as creating risks to the consumers who rely on their services. It is one of Government's core responsibilities to safeguard energy security and, given the evidence set out above, we do not believe that the market alone will drive adequate levels of cyber security.

We therefore propose that load controllers managing loads assessed by Government to have the potential to cause significant disruption to the sector are brought within the scope of the NIS Regulations. Through these regulations, load controllers would be required to take appropriate and proportionate security measures to manage risks to their network and information systems, report incidents that disrupt the continuity of the services to the relevant authority and take action to rectify those incidents. The application of the NIS regulations in the energy sector in Great Britain is based on outcome focused principles, using the NCSC developed Cyber Assessment Framework (CAF).

This approach does not prescribe compliance with specific standards, and instead focuses on proportionate risk management. In a nascent and evolving market, we consider this an appropriate method of regulation to limit the impact on emerging business models. Further information can be found in the BEIS Policy Guidance for the Implementation of the NIS Regulations[25].

BEIS and the Office for Gas and Electricity Markets (Ofgem) are designated as the joint Competent Authorities for the electricity subsector under the NIS Regulations. The Competent Authority is responsible for the implementation of the NIS Regulations, developing guidance for regulated organisations (Operators of Essential Services (OES)), overseeing compliance, and taking enforcement action (including issue of Information Notices, Enforcement Notices, or

[24] DCMS (2019) Cyber Security Incentives and Regulation Call for Evidence, https://www.gov.uk/government/publications/cyber-security-incentives-regulation-review-government-response-to-the-call-for-evidence

[25] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1022987/beis-policy-guidance-implementation-network-information-systems-regulations.pdf

Penalty Notices which can include a fine of up £17 million for serious breaches) where required. The security duties assigned to OES within the Regulations include:

- Taking appropriate and proportionate technical and organisational measures to manage risks posed to the security of the network and information systems on which their essential service relies. This includes ensuring a level of security of network and information systems appropriate to the risk posed.
- Taking appropriate and proportionate measures to prevent and minimise the impact of incidents affecting the security of the network and information systems used for the provision of an essential service, with a view to ensuring the continuity of those services.

The NIS Regulations also mandate the reporting of incidents affecting network and information systems which have a significant impact on the continuity of the essential service which the OES provides.

Thresholds

Under the NIS Regulations, a service provider is designated as an OES if its services rely on network and information systems and meets defined threshold requirements. The Government sets thresholds for different sectors and subsectors based on whether disruption to an operator's essential service could result in what the Government considers a significant disruptive effect. The current thresholds are set out in Schedule 2 to the NIS Regulations[26] for service providers in Great Britain that generate, transmit, distribute, or supply electricity.

In considering thresholds for load controllers, our starting point is to consider the scale at which a sudden shock (i.e. a large increase or decrease in electrical load) could impact on grid stability. Grid stability is managed by National Grid Electricity System Operator (NGESO). At any moment in time, available electricity supply must match fluctuating demand. Second by second, NGESO must maintain this vital balance to maintain overall system stability and prevent power disruptions. This is especially important with sudden changes in demand or generation, for example when everyone turns on their kettle at the end of a major sports event or popular television programme, or where a source of generation unexpectedly fails.

NGESO, in its role as System Operator in Great Britain, has statutory obligations to keep the System frequency between 49.50 – 50.50 Hz. If demand exceeds supply, the frequency of the electricity system will fall. If supply exceeds demand, the frequency will rise. The requirement for frequency response holding is calculated by NGESO. The minimum requirement is set to secure at 1260MW generation loss and/or 560MW demand loss based on the prevailing system conditions[27]. These levels could be increased above this to cater for specific loss risks.

NGESO considers a multitude of variables that influence demand, such as the weather, national events, when an interconnector will be exporting etc. to plan ahead and make

[26] https://www.legislation.gov.uk/uksi/2018/506/schedule/2/made
[27] https://www.nationalgrideso.com/industry-information/balancing-services/frequency-response-services (accessed 17 June)

informed decisions around the appropriate levels of frequency response to hold. To date, there has been a limited number of organisations operating within the electricity sub-sector capable of causing a significant enough demand loss to impact the network's stability. Such organisations have been limited primarily to interconnectors, currently in scope of NIS, and an emerging market of industrial aggregators contracted by the network operators. The NGESO has oversight of these organisations and is informed by agreement in advance of their activity, for example when an interconnector is due to export, as well as having real time visibility of the demand levels. This enables the NGESO to plan and ensure it is holding enough frequency response to maintain the system frequency in the event of unexpected changes in supply, such as a sudden stop in planned export by an interconnector.

However, NGESO will not have oversight of many load controlling organisations. A cyber-attack on a load controller could have an impact on the electricity system. Whilst NGESO may be able to manage a sudden loss under the threshold frequency response; a prolonged or fluctuating loss may have a broader impact on the stability and therefore functioning of the electricity system. This, combined with the ability of load controllers to remotely manage and optimise the flow of electricity to millions of devices in real time, sets them apart from traditional generation, transmission, distribution, and supply of electricity, introducing a new and growing risk.

For these reasons, we think organisations need to be managing their cyber security before they are managing the amount of load NGESO is securing against. **We therefore propose introducing new threshold requirements to ensure that organisations controlling loads at or above 300MW should be considered operators of essential services subject to obligations under the NIS Regulations.**

This consultation is an initial opportunity for input into these proposals. They will be developed further, informed by responses to this consultation, alongside additional risk assessment work that will be carried out with the NCSC and engagement with network operators and organisations currently controlling load. We will consult again at a later date on further developed proposals along with how the assurance and assessment approach taken will remain dynamic to future sector changes, including mechanisms network operators have in place for managing demand losses.

We invite your views on the following questions:

2. **Do you agree with the Government's proposal to make certain load controllers subject to the obligations in the NIS Regulations? Please explain your answer.**

3. **Do you agree with the Government's proposal of setting a threshold requirement of 300MW of remote load control for a load controller to be considered an operator of an essential service under the NIS Regulations? Please explain your answer and provide supporting evidence.**

4. **Are there any other threshold metrics that should be considered, for instance if organisations have more than a certain number of customers/appliances connected?**

An Outcomes Focused Approach

The Cyber Assessment Frame (CAF)[28] is widely used by Competent Authorities to assess compliance with the NIS Regulations. The CAF is an outcome focused cyber security framework, developed, and maintained by the NCSC. It consists of 14 principles which collectively represent a robust level of cyber security and resilience for organisations that provide vital services. These principles describe important outcomes that an organisation needs to achieve to successfully manage the risk of disruption to that organisation's essential functions caused by a cyber-attack or physical disruption to network and information systems.

Because the CAF is outcome driven and does not mandate how an organisation must achieve those outcomes, it enables flexibility. Organisations of different sizes and profiles can meet outcomes in a way that is suitable and proportionate to their own operations.

This methodology ensures that cyber risks are managed holistically, and that compliance is not a checkbox exercise. Most importantly, it promotes the management of risk within the organisation providing the service and avoids unintended consequences of prescriptive regulation environment in a nascent market.

The CAF breaks down each principle into a collection of more targeted cyber security and resilience outcomes which are used to assess the extent to which an organisation is meeting a particular principle. Each contributing outcome is associated with a set of indicators of good practice, the circumstances under which the contributing outcome is judged 'achieved', 'not achieved' or (in some cases) 'partially achieved' are described, and this is used to inform assessments of CAF returns from operators of essential services.

BEIS and Ofgem are joint Competent Authorities for the electricity sub-sector under the NIS Regulations. Both BEIS and Ofgem advise OES on organisation level expectations for meeting the CAF – appropriate to the sector and proportionate to the risk.

We propose to use the CAF to assess compliance for load controllers in scope of NIS. This enables an organisation level approach, scalable to a potentially diverse number of organisations operating in the market. It also supports a consistent approach to risk management and assurance and provides for comparability in understanding risks across operators of essential services under NIS. This is aligned with commitments in the UK Cyber Strategy to increase the adoption of the CAF or equivalents across CNI sectors and improve comparability with other cyber security assessment and reporting frameworks in use.

The CAF can also be aligned to other frameworks and standards and therefore allows users to translate language and certifications they are familiar with to the CAF.

5. **Do you agree with the Government's proposal of using the Cyber Assessment Framework (CAF) to support the implementation of the NIS requirements for load controllers? Please explain your answer.**

[28] NCSC (2019) CAF guidance, https://www.ncsc.gov.uk/collection/caf/cyber-assessment-framework

Next Steps

Further development of these proposals will be informed by responses to this consultation, alongside additional risk assessment work that will be carried out with the National Cyber Security Centre and engagement with network operators and organisations currently controlling load.

Subject to the will of Parliament, we plan to use regulation-making powers in new primary legislation – consulted on in Government's consultation on proposals for legislation to improve the UK's cyber resilience[29] earlier this year – to amend the NIS Regulations.

On the assumption that the new primary powers are secured to make the consulted-on changes to NIS, we will bring forward further consultation on a broader package of secondary legislation including further detail on the proposals set out within this document. As part of this, there will be additional proposals on how the Competent Authority will guide operators on meeting NIS requirements using the CAF, what appropriate assessment and assurance for load control looks like, and expectations of organisations that are captured within the scope of multiple requirements.

[29] https://www.gov.uk/government/consultations/proposal-for-legislation-to-improve-the-uks-cyber-resilience

3. Energy smart appliances: Outcomes

The purpose of this chapter is to establish the outcomes Government intends to promote in future policy for energy smart appliances (ESAs). It includes a summary of the objectives of these proposals and a description of how ESAs can be used to provide demand-side response (DSR). It describes the interoperability outcomes our proposals intend to achieve – including interoperability of ESAs with time-of-use tariffs and DSR service providers. Further outcomes relating to cyber security, data privacy and grid stability are also proposed.

The proposals within chapters 3 to 5 aim to enable greater uptake of DSR from domestic-scale ESAs, such as private EV charge points, batteries, and heat pumps. This chapter proposes specific outcomes across interoperability, cyber security, data privacy and grid stability that will inform future policy for ESAs. The following two chapters propose the specific technical and delivery frameworks required to deliver these outcomes in practice.

Increased uptake of DSR from ESAs would deliver benefits in three main areas:

- **Rewarding consumers for providing value to the energy system**, through enabling consumers to earn revenue or reduce costs, in exchange for providing DSR.
- **Reducing the overall cost of energy to all consumers**, through avoiding unnecessary network reinforcement and generation – reducing energy bills for everyone.
- **Reducing carbon emissions**, through shifting electricity demand to times where low-carbon electricity is more abundant.

ESAs can deliver DSR in different ways. At its simplest, an ESA could be scheduled to consume energy overnight, when overall demand on the electricity system is lower. Conversely, an ESA's energy usage could be remotely managed by a third party to reduce constraints of the local electricity network at short notice, whilst also delivering consumer requirements. While simpler forms of DSR are becoming more common today, more advanced forms of DSR are not adopted at scale. However, these more advanced approaches will be needed in the future to deliver the full benefits of flexibility to consumers and the energy system.

Approaches to DSR from ESAs can be categorised into different types, summarised in Table 3, below.

Table 3: Different types of DSR that could be delivered by Energy Smart Appliances

Type of DSR	Description	Example
Time-of-use tariff optimisation	ESA is configured to change when it uses or produces energy, in response to changes in the price of energy	ESA optimises energy usage against peak/off-peak tariff, or half-hourly 'dynamic' tariff that changes each day
Incentive data optimisation	ESA is configured to change when it uses or produces energy, in response to data (other than tariff)	ESA optimises energy usage based on published data for carbon intensity or wholesale energy prices
Local optimisation	ESA is configured to change when it uses or produces energy in response to energy usage, production, or storage of other appliances within the premises	ESA is optimised to consume energy produced by a solar panel in the consumer premises, co-ordinated via a Home Energy Management System (HEMS)
DSR services	ESA allows a third party to change when it uses or produces energy, typically to benefit organisations responsible for transmission, distribution, balancing or supply of electricity	ESA allows a third party to change when it uses energy to reduce the cost of energy supply, provide short term operating reserve, and/or manage a constraint on the local distribution network

With the right systems and standards in place, ESAs can provide DSR whilst still meeting consumer requirements, such as charging an EV by a certain time, or heating a home to a certain temperature. This can ensure the benefits of DSR can be accessed without significant changes to consumer behaviour or inconvenience.

To increase the uptake of DSR, ESAs will need to work with products and systems from different providers. This is referred to as 'interoperability'. Interoperability will ensure that consumers can use their ESAs for DSR with different service providers, and access different consumer propositions for DSR, without significant barriers (such as a need to replace or make a manual change to the ESA). Interoperability also provides a form of consumer protection, helping ensure consumers are not unfairly 'locked-in' if their preferences or circumstances change, or 'locked-out' from certain services or tariffs. Other risks from ESAs will also need to be mitigated, relating to cyber security, data privacy and grid stability.

Interoperability

A minimum level of interoperability is required to ensure consumers can use their ESAs for DSR with different service providers and access different consumer propositions. Government's approach is to prioritise interoperability for ESAs where there is a clear consumer and energy system benefit. **Government intends that future policy will ensure ESAs have the ability to:**

- **Receive and respond to time-of-use tariffs from different energy suppliers; and**
- **Provide DSR services with different DSR service providers.**

We do not propose requiring other forms of interoperability that unnecessarily increase costs or constrain market development and innovation. More specifically, we do not propose that any ESA must work with any user interface (i.e. an 'app') or third-party ESA operator. We are also not considering the interoperability of different devices within a home, including home energy management systems. Instead, our focus is on ensuring all consumers can access all tariffs and DSR services, regardless of the device they have.

Time-of-use tariffs

Time-of-use tariffs change the price of energy charged by an energy supplier, based on the time it is consumed or produced. Time-of-use tariffs will facilitate benefits to consumers and the energy system, through rewarding consumers for shifting consumption to times when supply of electricity is most abundant.

Most time-of-use tariffs are generally simple today, such as Economy 7 tariffs and other 'static' tariffs that do not change from one day to the next. However, Government expects that more suppliers will offer complex time-of-use tariffs in the future, as consumers and energy suppliers take advantage of smart metering and half-hourly settlement. This could include 'dynamic' tariffs, where prices for each time-period change more frequently.

Interoperability with time-of-use tariffs will ensure ESAs can receive and respond to tariff data from different energy suppliers, without significant manual configuration by the consumer. In practice, this requires energy suppliers to communicate this data in a consistent way.

The level of intervention required to enable interoperability of time-of-use tariffs is expected to be relatively low. However, time-of-use tariffs are typically a simple form of DSR, and are unlikely to deliver all the available benefits of DSR, such as when DSR is required at very short notice or in very specific locations. In addition, time-of-use tariffs may not be suitable for all consumers, particularly for more complex tariffs that are less common today. Other forms of DSR, described below, will also be required in the future.

DSR services

DSR services will allow consumers to delegate control of an ESA's energy usage or production, within the constraints of consumer preferences. This can enable third parties to reduce costs, such as wholesale costs incurred by an energy supplier. In addition, these third parties may use ESAs to participate in markets for DSR services, such as the Balancing Mechanism. This approach to DSR can be more sophisticated, allowing different energy system needs to be met in specific timescales and locations, potentially at short notice.

Interoperability will allow consumers to access a range of potential propositions from organisations acting as DSR Service Providers (DSRSPs), such as independent aggregators and energy suppliers, amongst others. Consumers will be able to access different benefits

from participating in these DSR services, such as financial remuneration or access to a discounted energy tariff.

Delivering this type of interoperability will require standardisation of the *minimum* functionality needed to deliver these services. This approach will enable ESA manufacturers (or permitted third parties) to maintain responsibility for the operation of the ESA, without placing unnecessary constraints on functionality that doesn't relate to DSR. This aims to maintain space for innovation, whilst reducing the scale of change and costs needed to deliver these outcomes in practice. It also allows international standards or approaches to be used for functionalities that are unrelated to DSRSP interoperability, if desired. Figure 1, below, illustrates how this approach could be delivered in practice, with a fuller explanation provided in Appendix 2.

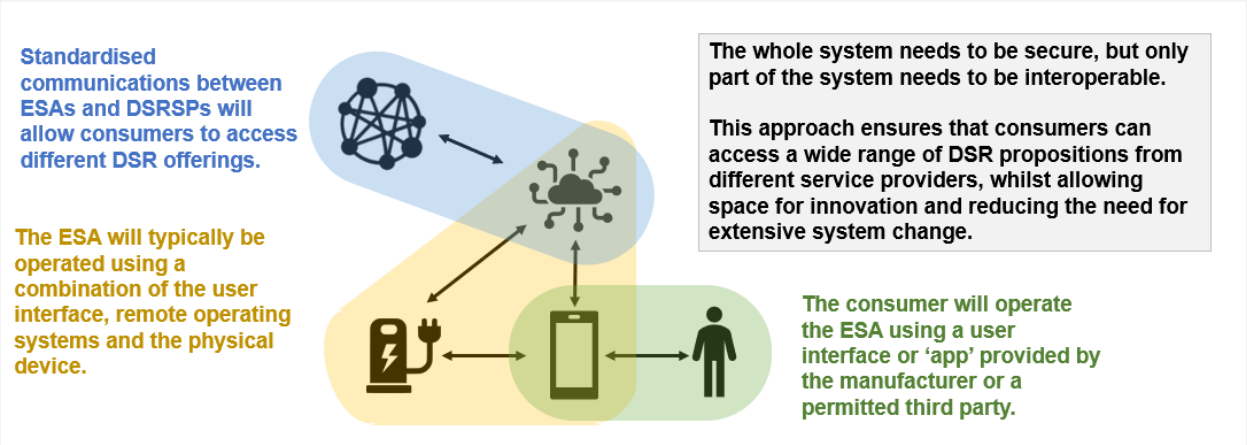


Figure 1: DSR Service Provider Interoperability - System Overview

Government also intends to work with industry to explore the potential of other approaches to DSR, whereby ESAs optimise their energy usage in response to published data other than tariff (referred to as 'incentive data optimisation' in Table 3). This will be facilitated through the governance arrangements described in Chapter 5.

6. **Do you agree with our proposed outcomes for interoperability? Please explain your answer.**

Cyber Security

As set out in the previous chapter, we propose that organisations controlling large amounts of load should comply with the NIS Regulations, to mitigate the most pressing cyber security risks to grid stability. However, Government also intends to protect against other risks, in addition to risks to grid stability from cyber security. This includes consumer detriment caused by loss of personal data, misuse of ESAs or loss of functionality. This recognises that any of these cyber incidents could damage consumer confidence in energy smart appliances, and adversely affect the uptake of DSR and low carbon technology.

To mitigate these risks, devices, organisations, systems and communications will need to be secure. Further requirements are likely to be needed for ESAs to reduce the risk of ESAs either being directly compromised or used to compromise other associated ESAs or systems. Additionally, adequate ESA cyber security protections will reduce the risks of ESAs being mis-used following the compromise of a connected system. However, it is also recognised that cyber security mitigations should avoid unnecessary constraints on innovation. They should still enable development of accessible, user-friendly ESAs that promote consumer engagement with DSR, without introducing disproportionate costs on ESAs or associated service providers.

Government is currently working with the National Cyber Security Centre (NCSC) to complete a risk assessment of the future system of ESAs and DSR. This will lead to more detailed cyber security requirements, developed in collaboration with industry. These requirements will be used to inform the technical frameworks and regulation of ESAs in the future. Based on work completed to date, Government has so far identified the following potential outcomes that ESAs may need to deliver:

- protect the integrity of messages and external data sources;
- protect against unauthorised access;
- protect against mis-use by authorised entities;
- mutually authenticate communicating entities and system messages;
- verify and validate all received data and messages;
- enable regular and urgent security updates, using secure update processes;
- protect the confidentiality of system messages, data-at-rest and sensitive processes;
- enable the detection of response to and recovery from compromise.

These high-level outcomes will be refined and potentially added to following further development of the cyber security risk assessment, described above. We expect industry to support this work through the governance arrangements described in Chapter 5.

7. What are your views on the initial proposed outcomes for cyber security of Energy Smart Appliances? Is there anything missing or not relevant?

Data Privacy

ESAs will have the potential to collect significant amounts of personal data, potentially at a high level of granularity. Requiring interoperability will require some of this data to be shared from the ESA to authorised DSRSPs, introducing new data privacy risks. Whilst UK-GDPR[30] and the Data Protection Act provides an over-arching regulatory framework for data privacy, any future technical solutions for ESAs (such as ESA standards) will need to ensure data privacy

[30] The provisions of the EU GDPR have been incorporated into UK law as the UK GDPR The UK GDPR merge the two pre-existing regimes for personal data protection, namely, EU GDPR and the 2018 Data Protection Act.

and data security risks are mitigated. Government proposes that future policy intervention should be designed in a way which:

- Avoids the unnecessary collection or transmission of personal data;
- Minimises the amount of personal data shared with third parties (including DSRSPs);
- Transmits and stores personal data securely, with controls in place to protect against access by unauthorised entities.

8. Do you agree with Government's proposed data privacy outcomes for ESAs?

Grid Stability

Increased uptake of ESAs presents both an opportunity and a challenge to grid stability. If operated in a smart and flexible way, ESAs can provide a valuable service to the energy system. However, recent analysis completed for 'Project REV' (Resilient Electric Vehicle Charging)[31] has identified a number of specific ways in which ESAs could also pose risks to grid stability, including:

- Synchronised changes in load ('herding') of ESAs at scale;
- Unexpected step-changes or ramps in energy usage at scale, in a short space of time;
- Oscillation in energy usage or production of ESAs at scale; and
- Inability to provide the flexibility necessary to the energy system, when depended on.

These risks could be caused by inappropriate design or configuration of ESAs (including their associated systems), misuse of ESAs, or consumer behaviour. To mitigate these risks, Government proposes that future policy should ensure that ESAs:

- protect against unintended synchronised changes in load (e.g. when responding to a time-of-use tariff or following loss of power or communications)
- enable load-impacting settings to be remotely updated over-the-air, ensuring they are not hard-coded into appliance firmware.
- collect and share data relevant for DSR and grid stability securely and reliably
- enable detection, alert and protection against anomalous load-impacting communications that could negatively impact grid stability

These outcomes intend to ensure that ESAs are manufactured with the capabilities to actively contribute to grid stability, identify risks to grid stability and mitigate these risks.

9. Do you agree with the risks to grid stability and proposed outcomes Government has identified? Is there anything missing or not relevant?

[31] ESC (2022) Resilient Electric Vehicle Charging: "REV", https://es.catapult.org.uk/report/resilient-electric-vehicle-charging/

4. Energy smart appliances: Technical frameworks

The purpose of this chapter is to set out the technical frameworks needed to deliver the outcomes proposed in the prior chapter. It includes proposals:

- For energy suppliers to make time-of-use tariff data openly available in a common format, over the internet
- For ESAs to meet regulatory requirements to meet interoperability, cyber security, grid stability and data privacy outcomes, through a standard based on PAS 1878
- For ESAs to meet minimum cyber security and grid stability requirements, similar to those already in place for EV charge points, in advance of these enduring standards

The previous chapter proposed a set of outcomes that future policy for ESAs will support. This included minimum interoperability outcomes, such that ESAs can be used with time-of-use tariffs from different energy suppliers, and for DSR services with different DSR service providers. Further outcomes relating to cyber security, data privacy and grid stability were also proposed.

In practice, delivering these outcomes will require several technical solutions to be developed and adopted. For ESAs to receive and respond to time-of-use tariffs from different energy suppliers, energy suppliers will need to make time-of-use tariff data available to ESAs in a common way. For ESAs to be used for DSR services with different DSR service providers, more substantive technical standards will need to establish how ESAs and DSR service providers communicate.

This chapter sets out proposals to develop and adopt the technical frameworks necessary to deliver the outcomes established in the prior chapter. This includes:

- **Data interoperability** – the approach to developing and implementing common data standards and data sharing mechanisms for time-of-use tariffs and other data used by ESAs for DSR;
- **ESA standards** – the approach to developing and adopting an enduring technical standard for ESAs that delivers interoperability, cyber security, grid stability and data privacy;
- **Minimum ESA requirements** – the minimum cyber security and grid stability requirements needed to ensure ESAs mitigate risks to consumers and the energy system in the near-term, in advance of enduring ESA standards; and
- **Common systems** – the shared systems and infrastructure that may be needed to ensure security and interoperability of ESAs.

The following chapter then discusses the overarching delivery frameworks needed, including the approach to implementation governance, demonstrating compliance and cost recovery.

Data interoperability

Time-of-use tariffs

ESAs will need to receive and respond to time-of-use tariff data, to optimise their electricity consumption or production on behalf of consumers. However, existing approaches to accessing time-of-use tariff data are not simple or consistent. Today, ESAs can access time-of-use tariff information by collecting it directly from a consumer, a smart meter, energy supplier websites and APIs[32], price comparison websites, and others. The lack of a reliable and consistent approach is a barrier to ESAs integrating with time-of-use tariffs, either requiring customers to manually configure their ESAs or for ESA manufacturers to build custom integrations with these data sources.

Most time-of-use tariffs available today are simple and "static", such that the prices and time periods are fixed for the duration of the contract. "Dynamic" tariffs – where the prices and time periods can change more frequently – exist but are not widely available. Over time, market-wide half-hourly settlement, and other regulatory reform[33] will incentivise energy suppliers to shift consumer demand to time periods where their costs are lower, using capabilities provided by smart metering. Consequently, "dynamic" tariffs are expected to become more common.

Whilst existing approaches to accessing time-of-use tariff data may be sufficient for simple tariffs, they are unlikely to be suitable for more complex tariffs expected in the future. Common data standards for time-of-use tariff information, and common ways to access this data, would make it easier for ESAs to use this data for DSR, and enable an improved consumer experience of time-of-use tariffs. In turn, this should help promote uptake of time-of-use tariffs, benefitting consumers and the energy system.

Government proposes to require energy suppliers, through an amendment to energy supplier licence conditions, to make time-of-use tariff data interoperable by being openly available in a common format. This should enable ESAs and their associated systems to access public time-of-use tariff data over the internet[34].

Subject to the outcome of this consultation, Government anticipates that this licence condition would be put in place as soon as is practicable. This recognises the immediate benefits of

[32] API or application programming interface is a type of software interface that provides a connection between computers or systems.
[33] In 2019, Government funded the Smart Tariffs – Smarter Comparisons project to demonstrate how smart tariffs can be compared by consumers - https://www.gov.uk/Government/publications/smart-meter-enabled-tariffs-comparison-project-smarter-tariffs-smarter-comparisons. Other reforms include Ofgem's review of electricity network access and charging, which will provide users with better signals about the costs and benefits they incur on the network at a particular time and place - https://www.ofgem.gov.uk/energy-policy-and-regulation/policy-and-regulatory-programmes/network-charging-and-access-reform.
[34] For avoidance of doubt, this does not include personal information about an individual consumer's energy tariff

increased time-of-use tariff uptake, and the expected increase in time-of-use tariffs following market-wide half-hourly settlement and increases in ESA adoption.

However, it is recognised that different technical solutions may be needed for more complex tariff types, such as 'dynamic' tariffs that must be updated more frequently. A phased implementation of these solutions may be appropriate, to unlock the benefits of interoperability for simpler, 'static' tariffs as soon as possible. If a phased implementation is taken, Government would ensure that energy suppliers could continue to offer innovative tariffs that might not be initially compatible with technical solutions, pending standardisation. For example, it may be that solutions for 'dynamic' tariffs take longer to develop and could potentially be exempt from these licence conditions initially.

The technical solutions to enable access to time-of-use tariff data could be developed and maintained under an industry code (such as the Smart Energy Code (SEC), the Retail Energy Code (REC) or the Balancing and Settlement Code (BSC)) or by Ofgem, Government or trade bodies. Given its existing role in data standardisation for smart metering, Government expects that the Smart Energy Code could provide appropriate governance to develop these arrangements.

Further into the future, consumers may want to share their *personal* tariff information (i.e. the specific tariff of an individual consumer) with other organisations. This could allow ESAs to integrate further with time-of-use tariff data, potentially updating tariff information when a consumer changes tariff or supplier. However, it also introduces data privacy and cyber security considerations. Organisations can currently access this data through the smart metering system, and Ofgem's midata project[35] could provide a secure mechanism for third parties to access personal tariff data over the internet. This project is currently on hold but may provide a longer-term solution, if re-commenced or continued in a different form. Government welcomes views on whether a longer-term solution to enable access to personal tariff data by third parties is required, and potential solutions.

For consumers to benefit from time-of-use tariffs, ESAs and associated systems will need to incorporate these into their functionality. In the first instance, we consider it makes sense to develop these solutions and to give industry time to consider and adopt these, ahead of reaching a decision on whether regulatory requirements are needed on ESAs themselves. However, Government could also include requirements for ESAs to integrate time-of-use tariffs in future ESA regulation, discussed in the following sections.

10. Do you agree with Government's proposals to make time-of-use tariff data openly available in a common format for Energy Smart Appliances?

11. Do you agree that the Smart Energy Code could provide the appropriate governance for development of common data standards? Please explain your answer.

[35] Ofgem Midata in energy programme, https://www.ofgem.gov.uk/energy-policy-and-regulation/policy-and-regulatory-programmes/midata-energy-programme (accessed 17 June)

12. How should Government ensure that Energy Smart Appliances integrate with time-of-use tariffs, beyond providing interoperability with tariff data?

Other 'Incentive Data'

ESAs could optimise their energy usage against 'incentive data' other than time-of-use tariffs. For example, National Grid ESO currently provide dynamic data relating to average carbon intensity of the energy system, for each half hour and region[36]. This data is made available via an API, enabling interoperability. This enables ESAs to optimise their energy usage to when carbon intensity is lowest, to minimise their impact on the environment.

Other potential data that might be used to optimise ESAs could include wholesale energy costs or network charges incurred by energy suppliers, amongst others. This approach could have similar benefits to time-of-use-tariffs, whilst allowing consumers to use single-rate tariffs and benefit from other forms of remuneration in exchange for providing DSR. This approach to DSR delivers benefits to consumers and the energy system. It may be possible to deliver interoperability of this type of DSR before other types of more complex DSR, potentially utilising similar technical frameworks to time-of-use tariffs. This would accelerate benefits of flexibility to consumers and the energy system.

This data could also be standardised, enabling ESAs to be interoperable with consumer propositions that take this approach to DSR. Requirements could also be needed on ESAs to establish how this data is received and understood, and to standardise any necessary communications back to the data provider. As part of ESA standards development process (described in the following section), Government will work with industry to consider whether further standardisation is required to enable interoperability of this type of DSR.

13. Should government consider standardisation of other types of 'incentive data' used by ESAs for DSR? Please consider what types of data and how they could be standardised.

Energy Smart Appliance standards

To meet the outcomes established in the prior chapter, ESA 'standards' will be required to establish how ESAs must operate and interact with DSR service providers. This section proposes the regulatory and delivery approach to developing and implementing these ESA standards. It also proposes the ESAs in scope of future regulatory requirements.

In a previous consultation[37], Government proposed smart metering as the lead option for the future smart charging architecture for EV charge points. This consultation looks at future requirements at the next level of detail – considering the component parts of future technical and delivery frameworks for smart, secure, and interoperable ESAs. Smart meters will continue to provide a foundational capability in the smart energy ecosystem, allowing consumers to

[36] Carbon Intensity API https://carbonintensity.org.uk/ (17 June 2022)
[37] EV smart charging consultation https://www.gov.uk/government/consultations/electric-vehicle-smart-charging

have greater control of their energy consumption and benefit from smart energy propositions, such as time-of-use tariffs, enabled through wider regulatory reform, such as Market-Wide Half Hourly Settlement. We also continue to substantively explore the potential re-use of cross-cutting security features and Smart Energy Code (SEC) governance in facilitating the implementation of our wider DSR policy, alongside other options. However, this consultation does not propose that the principal communications pathway between ESAs and DSRSPs must be over the smart metering system's communications infrastructure.

This recognises the prevalence of internet-connected appliances used today (domestically and internationally), and the impacts to ESA manufacturers from requiring communication to be through the smart metering communications networks. It also recognises the Government's view that sufficient security can be supported through communications networks used by ESAs today, if other mitigations are in place. However, the Government is continuing to consider the role of common systems required to deliver security and interoperability of ESAs, using internet-based approaches. Government intends to make use of established infrastructure and governance arrangements used for smart metering, where beneficial to do so.

Adoption

Technical standards are adopted at scale for a variety of reasons. Whilst commercial drivers and consumer demand can promote the adoption of standards, **Government proposes that regulation will be needed to promote adoption of ESA standards at scale,** to unlock the benefits of DSR from ESAs. We have considered the following options to promote adoption of ESA standards through regulation:

- **Option 1: Outcome-based regulatory requirements and 'presumption of conformity' through approved standards** – ESAs must meet outcomes established in regulation and are presumed to be compliant if they use a standard approved by Government or the regulator (sometimes referred to a 'designated' or 'deemed' standard). Other routes can be used to meet the required outcomes, that do not require use of an approved standard. However, organisations who do not use approved standards may need to meet other regulatory requirements, to demonstrate that the ESA meets the specified outcomes in a fair and robust way.

- **Option 2: Mandated standards** – ESAs must use a standard that is specifically mandated in legislation or other documentation, such as guidance or an industry code.

An outcomes-based regulatory approach, supported by approved standards (option 1), could allow a dominant standard to emerge, without preventing new approaches (such as international standards) being used. This could allow solutions to emerge that are lower cost or more effective, benefitting ESA manufacturers who may wish to adopt solutions that are most suited to their products. However, allowing choice between multiple standards could introduce complexity for DSRSPs who may need to support multiple approaches to be fully interoperable, and it is more likely to lead to circumstances where consumers find their devices are not fully interoperable. It also introduces more complexity for regulators.

These risks could be mitigated, through establishing appropriate regulations or governance. This could include requirements that ensure any non-approved standards used are robust, 'open'[38], do not create barriers to competition and allow appropriate assurance. Governance arrangements between industry, Government and a regulator could be required to facilitate approval of standards, ensuring all requirements are met in a fair and robust way.

Alternatively, a mandated approach (option 2) would provide greatest certainty that ESAs meet requirements. This could be simplest for DSRSPs to adopt, and for regulators to enforce. However, it could reduce the ability of industry to innovate, or to use suitable standards that emerge over time, before they are adopted in regulatory requirements. Similar to option 1, these risks could be mitigated through establishing appropriate regulatory or governance arrangements that allow emerging standards to be adopted, where appropriate.

Government has an open mind on whether Option 1 or 2 would be more suited to meeting policy objectives in practice. Government will need to consider potential trade-offs between accommodating innovation, and providing certainty that policy objectives are being met, amongst others. Government's focus for the short to medium term is to ensure a standard is developed that meets policy objectives and is ready to be used in a timely manner. We do not therefore consider that it is necessary or appropriate to take decisions on the optimal number of standards (i.e. one or multiple standards) at this juncture.

In all cases, Government expects to consider how any future regulatory framework can accommodate innovation and change, as existing standards evolve and new standards emerge – both domestically and internationally. This recognises that value to consumers, manufacturers and the wider energy system from maintaining alignment to the international markets and promoting adoption of the most effective technical solutions.

In addition, Government intends to consider the role of outcome-based regulatory requirements within the proposed regulatory framework. This recognises that outcome-based requirements may strengthen the obligations on industry to deliver policy outcomes, beyond just adopting the minimum requirements of a mandated or approved standard.

Government will consult further on the detail of this approach before introducing secondary legislation.

14. Do you agree that Government should establish regulatory requirements to promote adoption of ESA standards, and what would be your preferred approach? Please consider the advantages and disadvantages of an 'approved standards' (Option 1) vs. 'mandated' (Option 2) approach.

[38] 'Open' standards are typically developed in collaboration between all interested parties - not just individual organisations; developed using a transparent, published and robust process for feedback, ratification and decision-making; allow access to background intellectual property required for implementation on a fair, reasonable and non-discriminatory basis; and are well documented, publicly available and free to use.

Proposed Standards

In 2018, Government consulted on standards for ESAs and consequently commissioned the development of PAS ('Publicly Available Specification') 1878[39]. This standard was funded by Government, developed by industry, and coordinated by British Standards Institution. It was developed to resolve gaps in international standards, and to meet outcomes decided following consultation with industry. The first iteration of this standard was completed in 2021[40].

Government proposes that a standard based on PAS 1878 is used in future regulation of ESAs. This recognises alignment of PAS 1878 to our policy objectives (including the specific approach to DSRSP interoperability), alignment to emerging international standards, and the industry input provided during its development.

However, amendments or additions to PAS 1878 are likely to be required before it can be deployed at scale. Whilst we expect the high-level architecture and operating framework to be taken forward, Government welcomes industry proposals on what changes could be required in the future, to meet policy objectives in the most effective way. In addition, updates may need to consider regulatory changes, such as metering requirements for 'Virtual Lead Parties' participating in the Balancing Mechanism[41], and findings from demonstrations of PAS 1878, through Government's Flexibility Innovation Programme[42]. We anticipate that governance arrangements established for the next phase of standards development would provide a process for these additions or amendments to be proposed.

Government, supported by the National Cyber Security Centre, will work with industry to develop detailed security requirements and a future security architecture for ESAs. These requirements could also lead to additions or amendments to PAS 1878 being needed. Whilst these requirements develop, Government will continue to support the development of solutions for secure, interoperable DSR that re-purpose technology used for smart metering[43]. This anticipates possible future requirements for ESAs to use similar technologies and approaches, to provide robust security.

15. Do you agree that a standard based on PAS 1878 should be used in the future regulation of ESAs?

[39] Proposals regarding setting standards for smart appliances https://www.gov.uk/Government/consultations/proposals-regarding-setting-standards-for-smart-appliances
[40] BSI, smart appliances programme https://www.bsigroup.com/en-GB/about-bsi/uk-national-standards-body/about-standards/Innovation/energy-smart-appliances-programme/
[41] A number of modifications to the Balancing and Settlement Code and other associated documents have been made or raised that allow, or will allow, Virtual Lead Parties to participate in the Balancing Mechanism using BM Units that comprise equipment that is metered by "Asset Meters" which sit behind the boundary meter of the relevant premises. These "Asset Meters" could be contained within ESAs in the future, if they meet certain minimum requirements.
[42] Flexibility Innovation Programme https://www.gov.uk/government/publications/flexibility-innovation
[43] This includes supporting the development of PAS 1878 Annex D, and the specification for 'Standalone Auxiliary Proportional Controller' maintained within smart metering governance arrangements.

Energy Smart Appliances in scope

Government proposes for these regulatory requirements to apply to domestic-scale ESAs, including private (i.e. domestic and workplace) EV charge points, batteries, heat pumps, storage heaters and heat batteries. This reflects the high DSR potential of these ESAs and the expected scale of uptake in the coming years. This is proposed in addition to the regulatory requirements which already apply to private EV charge points, and other proposals in this consultation for other appliances, including minimum cyber security and grid stability requirements (in the following section) and minimum 'smart functionality (in Chapter 6).

Government will consider whether it is appropriate to extend these measures to other ESAs further in the future, such as wet/cold appliances and other Heating, Ventilation and Air Conditioning (HVAC) appliances not already in scope (such as air conditioning units). This recognises that the costs associated with these proposals may not be proportionate for ESAs with either expected lower uptake or less DSR potential. Government expects that a voluntary approach to adoption is a proportionate approach for these ESAs initially.

16. **Do you agree that Government proposals for ESA standards should apply to domestic-scale ESAs with the highest potential for flexibility, including private EV charge points, batteries, heat pumps, storage heaters and heat batteries? Please consider whether any other types of ESA should be in scope.**

Delivery approach

Further development of ESA standards will be required over the coming years. However, there are options for how standards development could be co-ordinated between organisations.

In all cases, it is anticipated that Government and the regulator will need to be actively involved in standards development. This includes establishing more detailed security requirements and providing ongoing assurance that policy outcomes are being met in a timely manner. However, our preference is to allow industry groups to take a leading role in standards development. This will promote ownership of the standard by industry in the long-term and promote accountability. However, industry will need to invest necessary time and resource to ensure standards development progresses at pace. If standards development does not progress at the required pace, Government may need to take a more leading role.

Government intends to ensure activity is co-ordinated by an entity who is independent (including sector- and technology-neutral), primarily UK based and experienced in multi-stakeholder standards development. Government would welcome views on two approaches in particular:

- **Option 1: British Standard Institution (BSI)** – as the UK's National Standards Body, BSI could develop the standard within relevant BSI committees and Steering Groups, and establish governance arrangements (such as industry working groups) to progress standards development. The standard could initially be maintained as a fast-track

'Publicly Available Specification' (as per PAS 1878) standard, and/or developed in to a full British or International Standard.

- **Option 2: Special-purpose industry group** - Industry could establish a special-purpose group to progress standards development. This could either be an informal working group (potentially facilitated by a trade association) or a special-purpose organisation with more formal governance arrangements (similar to Matter, the OpenADR alliance, Wi-Fi Alliance, or Open Banking Implementation Entity[44]). Industry would need to collectively provide resources to facilitate these arrangements.

Option 1 could utilise established standards development processes and governance used by BSI, whilst providing greater opportunity for alignment to international standards and World Trade Organisation requirements. It would also benefit from existing obligations on BSI to be sector- and technology-neutral, and to consider wider impacts of standards, such as consumer interests. This option may be quickest to implement, building on arrangements used for PAS 1878 and other British/International Standards.

Government also recognises that industry may prefer to build on approaches used in other similar sectors, where special-purpose groups have sometimes been established to progress with standards development. These groups could be supplementary to a BSI-led arrangements, with different approaches used to develop different aspects of the standard.[45]

Government is open to views on the preferred approach.

17. **What is your preferred option for developing and maintaining ESA standards in the future? Are there other options we should be considering? Please explain how you would expect your preferred option working in practice.**

Minimum ESA Requirements

A robust and proportionate approach to mitigate cyber security and grid stability risks from ESAs is required, to protect consumer confidence in DSR, mitigate risks to the energy system and avoid unintended consequences for consumers. This section discusses proposals to establish minimum ESA requirements, before enduring ESA standards are implemented.

Grid stability

As described in the previous chapter, ESAs can have a detrimental impact on grid stability through synchronised changes in load. The potential impact of synchronised response will grow as uptake of ESAs increases. These impacts could potentially be greater for types of

[44] https://csa-iot.org/all-solutions/matter/ and https://www.openadr.org/ and https://www.openbanking.org.uk/about-us/ (accessed 17 June)
[45] It is noted that the approach to PAS 1878 used BSI to develop the over-arching standard, whilst utilising a standardised solution from the OpenADR Alliance for the CEM to DSRSP interface.

ESA that are more likely to be configured to respond in synchrony, such as smart heating systems scheduled to turn on at 5pm.

From 30th June 2022, private EV charge points are required to mitigate this risk by applying a randomised delay to scheduled changes in electricity usage or production, of up to ten minutes. Exceptions are allowed where this is not appropriate or lower risk, such as consumer over-ride, or where a DSR service is provided. This aligns to the approach developed by industry and set out in the current version of PAS 1878. Similar requirements could also be put in place for other domestic-scale ESAs, including heat pumps, heat batteries, storage heaters and batteries.

Government welcomes views on whether grid stability mitigations are needed before enduring ESA standards are implemented, and whether randomised delay provides an appropriate mitigation. In addition, Government is open to views on alternative short-term mitigations to mitigate the risk of large-scale synchronised changes in load.

18. **Should Government mandate a randomised delay for ESAs, including heat pumps, storage heaters, heat batteries and batteries, to mitigate against risks to grid stability, in advance of longer-term ESA standards? Views are welcome on how a randomised delay could operate and on alternative mitigations.**

Cyber security

The proposals in the 'ESA Standards' section of this chapter will mitigate cyber security risks from certain ESAs. However, delivering these standards will take several years. Cyber security mitigations could be required sooner, to protect consumer confidence in ESAs, DSR and low carbon technology more generally. In addition, mitigations will reduce risks of ESAs being mis-used following compromise of an associated system, potentially risking grid stability.

The Product Security and Telecommunications Infrastructure (PSTI) Bill[46], currently in Parliament, will give Government the enabling powers to establish a regulatory framework to improve the security of consumer connectable products, following consultations by Department for Culture, Media and Sport (DCMS)[47]. The Bill sets out the scope of products that could be captured, including ESAs, whilst also allowing exceptions to the overall scope of the Bill through secondary legislation. It includes powers to introduce security requirements through secondary legislation and the Government has stated its intention that, initially, three requirements derived from ETSI EN 303 645 will be mandated. In addition, the Electric Vehicles (Smart Charge Points) Regulations 2021 will require private EV charge points to meet further minimum cyber security requirements also largely based on ETSI EN 303 645,

[46] The Product Security and Telecommunications Infrastructure (PSTI) Bill – product security factsheet https://www.gov.uk/guidance/the-product-security-and-telecommunications-infrastructure-psti-bill-product-security-factsheet

[47] https://www.gov.uk/government/publications/regulating-consumer-smart-product-cyber-security-government-response

recognising the increased cyber security risks. EV smart charge points will be exempt from the DCMS secondary requirements made under the PSTI Bill, to avoid duplication[48].

Government is considering whether some larger domestic-scale ESAs, including heat pumps, storage heaters, heat batteries and batteries, could need to meet minimum-security requirements prior to adoption of enduring ESA standards, beyond those proposed in the Product Security and Telecommunications Infrastructure Bill. This could establish good practice for technologies which pose greater potential risks to the energy system and minimise the number of less secure products placed on the market.

The ETSI 303 645 standard[49] is established internationally as a best-practice standard to mitigate low-sophistication cyber security risks to connected appliances. It has been used as the basis for future requirements Electric Vehicles (Smart Charge Points) Regulations 2021 and is also a requirement of the current version of PAS 1878. Requiring full compliance with ETSI 303 645 could ensure alignment across all ESAs in scope of these consultation proposals, whilst utilising an internationally recognised standard that should align to security requirements further in the future.

The specific requirements and enforcement approach could learn from the implementation of these requirements for private EV charge points[50]. BEIS will also continue to work closely with DCMS to ensure that businesses are not subject to unnecessary duplicative regulations across the measures being proposed for Energy Smart Appliances and for consumer connectable products more widely.

19. Should minimum device-level cyber security requirements be implemented for heat pumps, storage heaters, heat batteries and batteries, prior to implementation of enduring ESA standards? Should any other ESAs be considered?

20. Is ETSI 303 645 an appropriate standard for minimum device-level cyber security requirements for ESAs?

Common Systems

The proposals in the 'ESA Standards' section, and in Chapter 2, provide a baseline set of requirements for both ESAs and organisations. However, looking at any single component or function in isolation is likely to give an unbalanced view of security risks. Security of the whole 'system' will be required to sufficiently mitigate risks to consumers and the wider energy system, considering devices, organisations, communications, and systems. Common, shared systems or infrastructure may be required to mitigate risks across the system as a whole.

[48] https://www.gov.uk/government/publications/regulating-consumer-smart-product-cyber-security-government-response/government-response-to-the-call-for-views-on-consumer-connected-product-cyber-security-legislation
[49] ETSI EN 303 645 https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.00_30/en_303645v020100v.pdf
[50] The Electric Vehicles (Smart Charge Points) Regulations 2021, Schedule 1 https://www.legislation.gov.uk/ukdsi/2021/9780348228434/schedule/1

Government, working with the National Cyber Security Centre, is currently progressing a system-wide risk assessment for ESAs and DSR that will be used to inform future security requirements. This will consider whether common systems may be required to deliver adequate security, whilst ensuring interoperability. This section puts forward initial considerations to illustrate three areas where common systems and infrastructure could be required: Public Key Infrastructure (PKI), anomaly detection and communication networks. This section also discusses the approach to delivering common systems, if needed.

Public Key Infrastructure

The practical implication of requiring interoperability is that ESAs must be able to securely communicate with a range of service providers in a common way. The most common security control used to enable this is 'Public Key Infrastructure' or PKI. PKI is a system of processes, technologies, and policies used to enable encryption and authentication, using digital certificates to verify the identity of appliances and service providers[51]. It is often the preferred approach in ESA standards (including PAS 1878) to ensure communication is secure.

PKI providers will be delivering services that are depended on by consumers and the energy system. If a PKI provider were compromised, this would introduce significant risks to both consumers and the energy system more widely. Given these potential impacts, it is important that any approach to PKI is robust, and PKI providers are suitably secure.

Government, supported by NCSC, will work with industry to develop a security architecture that establishes the role of PKI within an interoperable DSR system for ESAs. Arrangements may be required for specified PKI service providers to provide the necessary certificates, and to operate in a secure manner. These interventions could include potentially limiting this role to a single service provider, where there is a clear security, interoperability, or cost benefit.

Anomaly detection

If a load controller was compromised through a cyber-attack, controls may be needed to prevent impacts on grid stability. These impacts include ESAs changing their energy usage or production in aggregate. One security control that can help to mitigate these risks is 'anomaly detection'. Whilst there are different variations in how anomaly detection can be implemented in practice, it often involves performing checks on the volume, frequency and/or contents of messages, to identify unusual or suspicious patterns. If so, system users can be alerted, and potential impacts can be mitigated appropriately.

As ESAs will need to be operated by multiple potential DSRSPs, anomaly detection could need to be applied in an interoperable, common manner. If anomaly detection from a third-party system is needed, requirements could be needed to ensure those systems are secure, given they are providing a service that grid stability is dependent on.

[51] A more comprehensive description of PKI is provided by NCSC: https://www.ncsc.gov.uk/collection/in-house-public-key-infrastructure/introduction-to-public-key-infrastructure

Government, supported by the NCSC, will work with industry to develop security requirements and a security architecture that ensures risks to grid stability from cyber-attack are identified, alerted, and protected against in a robust way. This will consider different approaches to anomaly detection, such as through common systems or further appliance/organisation requirements.

Communications networks

Government has considered the role of communications networks used by ESAs and organisations who communicate with them. These communications networks are often described as 'local' (i.e. over a short distance) and 'wide' (i.e. over a long distance). Today, many ESAs use internet in the consumer premises to communicate remotely. However, private communication networks, such as the smart metering home/wide-area network, can also be used. These different communications networks will introduce different cyber security risks. There are also relevant interoperability, availability, and latency considerations.

Government does not expect to prescribe a local- or wide-area communication network for ESAs. In practice, this will allow ESA manufacturers to have a choice of communications networks, providing that interoperability can be delivered. Our expectation is that prescribed communications networks, such as those used for smart metering, are not needed to sufficiently protect risks to grid stability, provided that other mitigations are in place. However, future security requirements may result in requirements on communication networks.

21. Do you agree that common systems could be required to mitigate system-wide risks? What issues will need to be considered in the design of such systems?

Delivery approach

If common systems are required in these areas, there are several approaches to deliver these:

- **Option 1: Extend the role of the Data Communications Company (DCC) –** Government or Ofgem could change the DCC licence and potentially the Smart Energy Code to include required activities. New or existing service providers would be appointed to provide required systems, using internet-based communications.
- **Option 2**: **Create a new licensed common service provider –** Government or Ofgem could establish a new licence for a common service provider, with supporting governance arrangements to manage cost and performance. A new licence-holder would be competitively appointed to fulfil its functions.
- **Option 3**: **Establish a new body to procure common systems –** Government, Ofgem or industry could create a new not-for-profit company responsible for delivering

capabilities needed and supporting governance/cost recovery arrangements. This body could procure common systems (and other shared services) where needed. [52]

- **Option 4: Establish a list of 'approved' service providers** – Government of Ofgem could establish security and technical requirements for common service providers and allow any service provider that meets those requirements to be used.

Government anticipates that creating a new licensed common service provider (option 2) is likely to require significant regulatory change, taking several years[53]. Government's view is that this is unlikely to be preferable to extending the DCC licence, given the similar role of DCC in smart metering today. On this basis, Government proposes to discount Option 2. The suitability of other options will depend on the nature of the common systems required, and the exact requirements that any common service provider may need to meet. If extensive, highly bespoke systems are required, Option 1 may be more desirable, given the similar role of DCC in smart metering, and potential time saved from using existing arrangements. However, the scale of regulatory change needed could be significant. If less bespoke systems are required, Option 3 or 4 may also be viable, but may also require significant regulatory change.

Further development of security risk assessment and security requirements will be required before understanding the suitability of these options in full. As such, Government proposes to keep Option 1, 3 and 4 open, whilst this work progresses further.

22. What issues will Government need to consider when reaching a decision on delivery approach for common systems?

[52] The new body could be established along the lines of RECCo or SECCo and would be governed under an industry code, rather than being directly licensed. It may also be possible to re-use an existing central body that has already been established.

[53] More specifically, it would require Government and/or Ofgem to establish a new licensable activity through primary legislation, consult on and issue a new licence, competitively appoint a new licence-holder and establish its governance arrangements.

5. Energy smart appliances: Delivery frameworks

The purpose of this chapter is to set out how the technical frameworks for secure, interoperable ESAs will be delivered in practice. It seeks views on the overall approach to implementation governance during the different phases of the delivery, how ESAs could demonstrate compliance and how the costs of these activities could be recovered.

This section considers the over-arching delivery frameworks required to deliver the policy proposals and technical frameworks discussed in Chapters 3 and 4. It specifically considers **implementation governance, demonstrating compliance**, and **cost recovery**.

Implementation Governance

Over the coming years, Government, regulators and industry will need to work together closely to deliver the policy outcomes outlined in this consultation. Key activities could include:

- Developing, testing and maintaining a standard for ESAs;
- Developing common data standards for time-of-use tariffs and other data for DSR;
- Developing test specifications;
- Establishing assurance schemes;
- Procuring, designing, developing, testing, and implementing common systems; and
- Policy development of new regulations and contractual arrangements between ESA manufacturers, DSRSPs and central service providers.

The following section describes how Government, regulators and industry could work together to deliver and govern these activities in practice. We expect these arrangements to evolve over time, but, broadly speaking, expect there to be three phases of delivery:

- **'Development' phase:** the period during and immediately following this consultation, during which future governance arrangements and plans are designed and mobilised.
- **'Transition' phase**: the period before the actual manufacture and sale of compliant ESAs, during which ESA specifications, assurance schemes, central services and contractual arrangements will be established in full.
- **'Delivery' phase:** the long-term arrangements during and after the manufacture and sale of compliant ESAs, during which standards and contractual arrangements need to be maintained, ESAs need to demonstrate compliance and common systems could need to be used and maintained.

'Development' phase

In tandem with this consultation, Government will establish arrangements to mobilise and accelerate the activities needed to deliver. The key focus areas are anticipated to include:

- **Engagement** – Maintaining alignment of stakeholders to the strategy and delivery approach and allowing industry to provide strategic direction where needed.
- **Coordination** – Developing, sharing, and assuring plans, and coordinating inputs.
- **Governance** – Progressing design and delivery of governance arrangements required during the 'transition' phase and managing effective handover to these arrangements.
- **Technical design** – Identifying amendments or additions to ESA standards and other technical artefacts, to be delivered during the 'transition' phase.
- **Security** – Development of security risk assessment, requirements, and architecture, including potential common system impacts (such as PKI and anomaly detection).

Government anticipates initially establishing and chairing an industry working group to begin these arrangements. Industry participants and trade bodies would be invited to support development of plans, technical documentation, and future governance arrangements. This group would be flexible in remit and able to create further working groups with specific focus areas, ensuring the correct industry representatives can input to relevant discussions at pace.

Government would aim to hand over responsibilities to 'transition' governance arrangements as soon as practical, working with industry to make sure this is set up and mobilised effectively. This handover could be phased, with certain groups transitioning sooner than others.

'Transition' phase

The objective of the 'transition' phase is to establish the essential capabilities needed to provide consumers with secure, interoperable, and compliant ESAs in full. Relevant activities during this phase could include developing, testing and iterating a working ESA standard, establishing assurance regimes, establishing common systems, drafting legislation and agreeing any contractual arrangements between parties, amongst others. Government, regulators and industry will need to work together jointly during this period, taking different roles on different aspects of delivery.

A central delivery and governance function could be needed to ensure all aspects are co-ordinated effectively. The central function may be required to deliver activities relating to:

- Facilitating steering groups and working groups;
- Establishing scope, plan and objectives of delivery activities, and appointing service providers to deliver these activities;
- Engaging and co-ordinating stakeholders across industry and Government;

- Facilitating procurement and contract management of common systems or service providers;
- Developing and managing against an over-arching delivery plan; and
- Creating and maintaining budgets, and facilitating cost recovery from relevant organisations.

Government anticipates that any central function would need to meet the following principles:

- **Accountable** – appropriately incentivised for the successful delivery of its objectives.
- **Cost-effective** – delivered at a cost that is proportionate to the benefits to consumers.
- **Deliverable** – able to deliver the required outcomes in the time required.
- **Scalable** – able to deliver the range of activities required, at the necessary scale.
- **Representative** – able to fairly represent the needs of the range of impacted stakeholders, such as electricity network/system operators, ESA manufacturers, DSRSPs, Government, regulators and consumers.

The exact role of any central delivery function will be dependent on the technical solution, and particularly the role of common services that could require procurement. Overall, Government expects that more formal structures will be required during this phase, with robust governance established through regulations, corporate governance or contracts, and the capability to procure common services on behalf of industry. Informal arrangements, potentially consisting of working/steering groups and service providers contracted by government, are unlikely to be sufficient to deliver the outcomes required – particularly if extensive common systems or services need to be procured on behalf of industry,

Government has considered two options for governance arrangements during this phase:

- **Option 1**: **Establish central, not-for-profit, delivery body -** Government, regulators or industry would establish a new not-for-profit body, responsible for delivering required outcomes. Government, regulators or industry would establish its governance, establish a cost recovery mechanism and appoint service providers and staff to deliver its functions. This body could be jointly owned by industry, with the flexibility to adapt the scope and delivery approach to meet the needs of its stakeholders. This could be established in a manner similar to SECCo or RECCo in the energy sector. Similar approaches from other sectors, such as the Open Banking Implementation Entity[54], could also be relevant.
- **Option 2**: **Build on existing Smart Energy Code governance arrangements –** Government or Ofgem could amend the SEC and DCC licence, amongst others, such that the SEC governance and delivery structures can be extended for these purposes. Existing arrangements could be extended where appropriate, and new arrangements

[54] Open Banking https://www.openbanking.org.uk/about-us/ (accessed 17 June)

within existing governance could be established. For example, secretariat functions could be extended, whilst new ESA-specific codes could be created.

Option 1 would be flexible and scalable for our needs, adapting its scope, size, governance and delivery approach over time as needed. However, this could require more cost and time to establish. It could also create a risk of additional longer-term overheads, on both Government and industry in terms of time and funding commitments. There could also be a risk of some duplication in roles and functions between any new body and existing ones. The additional time to establish a new body could impact when technical solutions could be implemented.

Option 2 would benefit from re-using existing arrangements from a similar sector, potentially saving costs and time compared to establishing new arrangements. This could be particularly beneficial if extensive common services or systems are required in the future, given the procurement and contract management capabilities established for SEC governance. However, the scale of change required to existing SEC governance could be high, mitigating these benefits in part.

Government proposes to work with industry during the 'development' phase to develop and assess Options 1 and 2 further.

'Delivery' phase

The delivery phase includes the activities during and after the manufacture and sale of compliant ESAs. This consultation does not propose these arrangements in any detail, given the significant amount of time before these arrangements must be in place, and dependencies on other policy decisions discussed elsewhere in this consultation.

Government expects these arrangements would follow precedent in other sectors where industry (or bodies delegated by industry) take responsibility for delivery. Regulators would monitor compliance and take enforcement action where needed. Government input would be reserved for issues of special interest, such as national security or strategic change.

Potential activities required during this phase could include:

- Maintaining ESA standards and other technical documents;
- Contract management and ongoing delivery of common services, if required;
- Delivery of assurance schemes, including potential testing capabilities;
- Change control for any contracts between organisations;
- Identifying and resolving strategic, cross-cutting issues; and
- Monitoring and enforcement of regulations.

In practice, these activities will require governance in some form, including agreed processes for managing change and ensuring effective delivery of any common systems or services. As is described in the prior section on the 'transition' phase, Government is considering different options to deliver and govern these activities. This includes considering whether to amend and

extend Smart Energy Code governance for these purposes or create a new industry-owned central body responsible for these activities. However, the exact nature of the arrangements during this phase will be highly dependent on other policy decisions, including the role of common systems and the enduring body responsible for maintaining standards.

23. What are the key considerations for design of governance during the development, transition and delivery phases of implementation?

Demonstrating Compliance

This section invites views on how different economic actors (such as manufacturers, importers, distributors, wholesalers and retailers) in an ESA supply chain could provide assurance that their products meet the proposed regulations described in the previous chapters.

Assurance

An appropriate and proportionate ESA assurance scheme will be necessary to ensure consumers, industry and Government can be confident that appliances meet the required outcomes, when they are placed on the market. In general, assurance approaches can vary in their complexity and scope. Government recognises that the future approach to assurance must be proportionate to the risks that non-compliant ESAs could pose to consumers and the energy system. The impacts and costs to businesses undertaking the assurance activity will also need to be considered.

At a high-level, Government considers the following assurance options to be available for device-level assurance:

- **Option 1: Self-certification without testing** – Under this option, no mandatory testing obligations are in place. Instead, there is a mandatory requirement that documentation should be made available to the enforcement authority upon request, such as a technical file, which can demonstrate how appliances meet the regulatory requirements.
- **Option 2: Self-certification with testing** – Under this option, there are mandatory testing obligations, where appliances are required to be tested against the various technical regulatory requirements.[55]
- **Option 3: Third-party certification with testing** – Under this option, testing could be applied as per option 2, with the addition of test results supplied to an accredited third-party certification body. Approval from a certification body would be a pre-sale requirement to allow products to be placed on the market.

Whilst the above options are relevant for device-level assurance, Government also recognises that assurance of relevant supporting systems or platforms (such as ‘cloud’ based systems) could be required, particularly where they have the potential to impact policy outcomes, such

[55] There are several variations of this approach. For example, the testing obligation may require outcomes-based or rules-based testing (i.e. using a standardised testing specification), allow in-house testing, or mandate that it must be completed by an accredited independent testing house.

as interoperability or security. Government welcomes views on how assurance of these systems could need to be delivered, alongside device-level assurance.

Assurance schemes will need to evolve over time. This will be impacted by how standards, regulations, the market, and the risks change over time. Governance of any related standards and scheme would be needed to manage this ongoing process. Government will need to consider how this could operate and who would be best placed to oversee any assurance scheme.

Taking a risk-based approach to assurance may mean some requirements will require a greater level of assurance than others. This includes cyber security requirements that protect critical national infrastructure. A robust and proportionate approach to assuring cyber security requirements will be needed to provide confidence that security risks are being mitigated. A different approach to assurance could be required for the proposals in the 'Minimum ESA requirements' section, compared to those in the 'ESA Standards' section.

Whilst 'Security Characteristics' and 'Commercial Product Assurance' (CPA) is used to provide security assurance in smart metering, NCSC have phased out CPA for all other products and proposed a Principles-Based Assurance[56] approach to future technology assurance. This approach proposes several flexible security principles to be assured against, including design and functionality, product development and through-life assurance.

Government expects ESAs to require a robust but proportionate approach for demonstrating compliance with cyber security requirements, potentially using third-party testing and certification. At present, Government is considering whether this would be part of NCSC's future Principles-Based Assurance scheme. Government expects to continue to engage with industry to develop the approach to assurance of security requirements further.

Government also recognises that more substantive assurance arrangements may be needed for interoperability, to provide confidence that appliances operate with different DSRSPs as intended. This could include testing of appliances with DSRSP systems. For other requirements, such as grid stability and data privacy, Government has an open mind on how assurance could be delivered in an appropriate and proportionate way.

Proposals for how to effectively enforce the ESA requirements are still under consideration and Government will consult on its approach later, ahead of implementation. Government anticipates that future legislation would broadly align with the enforcement approach adopted in existing product legislation, providing any enforcement authority with a range of enforcement tools to ensure it can investigate and take remedial action against non-compliance.

24. Are there any considerations Government has not mentioned that should be factored into future policy on assurance? Please consider assurance for devices and associated systems, such as 'cloud' platforms.

[56] NCSC, Technology assurance, https://www.ncsc.gov.uk/collection/technology-assurance/future-technology-assurance

25. What is your preferred approach for assurance for ESAs, and why? Please provide any evidence on the relative impacts, costs, and benefits of different approaches.

Labelling

Government is considering the value of introducing a labelling scheme for ESAs in and out of scope of the regulatory requirements proposed in the prior chapter. A labelling scheme could enable consumers to make informed decisions at point of sale, promoting consumer uptake of ESAs with DSR functionality, and encouraging the market for DSR to grow. This could, in turn, unlock further system-wide benefits from DSR, benefitting all consumers – particularly from ESAs that are not subject to regulatory requirements. Government previously consulted on the potential of a labelling scheme in 2018, within the consultation on ESAs, and there was no consensus on the preferred approach.

Labelling could be used in a variety of forms to help engage consumers in ESAs and DSR. This label could indicate the functionality provided by the ESA, the expected consumer benefits from DSR, or compliance with specific regulatory requirements. It could be implemented on a voluntary basis, through an industry code, or supported by legislation establishing when and how it could be used.

At this stage, Government is still considering the merits of introducing a labelling scheme. We are also considering the potential to extend the role of existing energy labelling schemes, potentially through incorporating smart functionality into the overall energy efficiency rating of ESAs. As we take the policy forward and consult further, we will consider options to extend existing energy labelling schemes and to develop a stand-alone label.

26. Do you think a labelling scheme for ESAs could help promote consumer uptake in DSR from ESAs? If yes, what type and form of labelling would be most beneficial?

Cost Recovery

It is Government policy that public sector organisations should charge for publicly provided goods and services based on full economic cost recovery, where possible[57]. Full cost recovery means ensuring the full cost of delivering a service, product or project, including the relevant proportion of overhead costs, is recovered.

The activities required to deliver these policy objectives will incur costs that will need to be recovered appropriately. The scale and type of these costs is highly uncertain at this stage, given the low maturity of the technical solution and delivery frameworks. It is therefore challenging to propose a preferred approach to distribute and recover costs, independently of other policy decisions. However, there are different approaches to distribute and recover costs, which will impact end consumers in different ways:

[57] HMT (2012) Managing Public Money, https://www.gov.uk/Government/publications/managing-public-money

- ESA manufacturers – via cost of ESAs
- DSR Service Providers – via costs or reduced revenues from DSRSP consumers
- Energy system/network operators (such as the transmission, distribution and/or future system operators) – who may then in turn seek to recover costs.
- Energy suppliers – who may then pass costs on to consumer energy bills
- Government – via general taxation on all consumers

In practice, these options are not mutually exclusive. Different costs could potentially be recovered from different actors during different phases.

During the 'development' phase, costs could be associated with establishing and supporting working groups. As is the case for normal policy development activities, Government and industry would fund these activities through business-as-usual arrangements.

During the 'transition' phase, costs could be associated with ESA standards development and testing, test specification development, assurance scheme set-up, procurement and implementation of common systems, and delivery of any central governance arrangements. There is precedent for these costs to be borne primarily by those participating in these arrangements (i.e. ESA manufacturers and DSRSPs). However, Government is also mindful of potentially placing a disproportionate cost burden on 'early movers' in the sector, potentially to the benefit of other organisations who join the market later and avoid these initial costs. Whilst recovering these costs from other groups (such as through network or energy supplier charges) would mitigate this impact, it would pass these costs on to consumers who do not directly benefit from these policy proposals.

During the 'delivery' phase, costs could be associated with maintenance of ESA standards (and other similar documents), maintenance of governance arrangements, delivery of assurance schemes (including ESA testing), and delivery of central systems, amongst others. There is precedent for the costs of these activities to be recovered from those participating in these arrangements (i.e. ESA manufacturers and DSRSPs).

Government's view is that the costs of these arrangements should be recovered from those ultimately benefitting from these arrangements, accountable for their successful delivery and incentivised to obtain value-for-money. This would predominantly include ESA manufacturers and DSRSPs who develop products and services through these arrangements. It could also include energy system/network operators who could earn new revenues from increased market for DSR services, and avoid costs of system reinforcement from increased flexibility. Government expects that funding all arrangements predominantly through Government grants is unlikely to be suitable. Other options will be considered in more detail following further development of the technical frameworks and governance arrangements.

27. What factors should government take account of when considering how the costs of delivering these arrangements should be distributed and recovered?

6. Smart Electric Heating

This chapter sets out our proposed approach to mandating smart functionality for certain electric heating appliances. It seeks views on the appliances in scope, the definition of smart functionality for the purpose of the mandate, and the timing of implementation.

In addition to ensuring all Energy Smart Appliances (ESAs) meet the proposed interoperability, cyber security, grid stability and data privacy outcomes described in the previous chapters, Government has specific ambitions to increase the number of electric heating appliances with smart functionality.

Increased uptake of electric heating with smart functionality will help reduce heating running costs for consumers and minimise the need for wider electricity network reinforcement and generation capacity, by reducing peak demand. Alleviating pressure on the networks from the electrification of key sectors such as heating and transport will also support the networks' critical role in safeguarding our energy security.

Therefore, Government is proposing a "smart mandate" which will require electric heating appliances with the greatest flexibility potential, namely heat pumps, storage heaters, and heat batteries, to have smart functionality. This will ensure that all consumers with these appliances can use them in a smart and flexible way.

Context and rationale for intervention

Heat in buildings accounts for 23% of total emissions in the UK. Reducing greenhouse gas emissions to net zero will therefore require virtually all heat in buildings to be decarbonised. There are several strategic pathways to decarbonise heat by 2050, with a range of low-carbon technologies and systems that may have an important role to play, including heat pumps, heat networks and potentially hydrogen for heating. However, the electrification of heat is the only currently proven option for the decarbonisation of buildings at scale, and highly efficient electric heat pumps will form a major part of how we heat our buildings in all future scenarios.

As set out in the Heat and Buildings Strategy, we are aiming to deploy at least 600,000 heat pumps annually by 2028[58]. This level of heat pump deployment is strategically important in all potential routes to net zero, even in a scenario where much of our heating comes from hydrogen in 2050, and it is essential for ensuring an electrification-led route remains viable. This would require further growth to much higher numbers of annual heat pump installations by the early 2030s.

[58] BEIS (2021) Heat and Buildings Strategy, https://www.gov.uk/government/publications/heat-and-buildings-strategy

Around 55,000 heat pumps were installed in the UK in 2021, and a rapid scale up of deployment is needed. In the Heat and Buildings Strategy[59], Government set out a package of policy measures to deliver this transition in a fair and affordable way. This includes the Boiler Upgrade Scheme, which opened in April 2022, and proposals to introduce a market-based mechanism for low carbon heat from 2024, as well as regulations to phase out the installation of fossil fuel heating in off gas grid buildings. We are also introducing regulations in 2025 to ensure that all new build homes have low carbon heating, predominantly heat pumps.

We recognise that there is a growing electric heating market beyond heat pumps and understand that the transition to net zero may require several options for consumers and businesses both and on and off the gas grid. Alternative electric heating appliances such as storage heaters – which already typically use a 'static' time of use tariff, such as Economy 7, switched via the Radio-Teleswitch Service (RTS), or smart meters – may have a future role to play. However, given they typically use more energy than a heat pump to meet the same heating demand, we expect this to be limited to specific use cases such as small flats.

In any case, the scaling up of the electrification of heat, alongside transport, will increase demand on the electricity networks. In addition to this, electricity generation will become increasingly variable, dependent on the time of day, season, and weather conditions, as well as more decentralised, as the UK continues to connect more renewables to the grid.

These are necessary outcomes of the shift away from fossil fuels to low-carbon energy sources. They highlight the importance of ensuring that electric heating appliances have the capability to support a smart and flexible energy system which underpins energy security and helps us meet our net zero targets.

Electric heating appliances with 'smart' functionality will be able to provide flexibility, through changing when they use electricity in response to the needs of the electricity system. Like other ESAs, as set out in Chapter 3, increased uptake of Demand Side Response (DSR) from smart heating appliances will benefit both consumers and the network by: rewarding consumers for providing value to the energy system; reducing the cost of energy to all consumers by avoiding unnecessary network reinforcement and generation; and reducing carbon emissions. Smart functionality could also provide consumers with greater control over how they heat their home. We acknowledge that some consumers, such as low income or vulnerable consumers, may require additional support to realise the benefits of smart heating.

We anticipate that the addition of smart functionality may result in a small increase[60] in the upfront cost for the technologies included in the scope of the proposed mandate. However, it is

[59] BEIS (2021) Heat and Buildings Strategy, https://www.gov.uk/government/publications/heat-and-buildings-strategy

[60] We estimate an additional cost of £40-£100 to make a heat pump complaint with the proposed smart mandate. At this stage we've used evidence from smart EV charging points to infer about the likely cost per unit, assuming that the hardware and software requirements for smart functionality will be similar. This suggests an additional unit cost of £40. A sensitivity assumption of £100 per unit is assumed based on market review of current retail price of heat pump smart controls. This is compared to current total installation costs ranging from £7,000 to £14,000 for domestic housing types today installing an air source heat pump, with the aim for cost parity between heat pumps and gas boilers by 2030 and significant cost reductions of at least 25-50% by 2025. The exact costs Will be driven by the precise details of the standards and functionality requirements set out in secondary legislation.

critical to help deliver bill savings for consumers. Alongside steps Government is taking to reduce heating demand and help rebalance electricity and gas prices, this will support work to make heat pumps no more expensive to run than boilers by the end of the decade.

Appliances in scope of the mandate

The mandate would initially apply to electric heating appliances with the greatest potential to be used flexibly (i.e. with the greatest ability to shift demand for electricity). On this basis, the initial cohort of appliances that are proposed to be mandated to be smart is hydronic heat pumps, storage heaters and heat batteries. The proposed capacity limit for the mandate, and definitions for the individual appliances are as follows:

Capacity limit: Domestic-scale appliances (up to 45kW rated thermal capacity) which provide space heating and/or sanitary hot water as part of a central heating system. This includes domestic scale heating appliances for use in non-domestic buildings.

Hydronic heat pump: A heating appliance that extracts low temperature heat from a renewable source such as the air, water or the ground and upgrades it to higher temperature heat to feed a central heating and/or a sanitary hot water system. This includes the hydronic heat pump element of any hybrid heating system which combines an electric heat pump with a combustion boiler using fossil fuels or low-carbon alternatives.

Storage heater: An established space heating appliance that can be used flexibly to utilise periods of cheap and clean electricity generation by using electricity to heat a solid storage medium which can be discharged to provide heating during peak demand.

Heat battery: An emerging electric heating appliance that can be used flexibly to utilise periods of cheap and clean electricity generation by using electricity to heat a thermal storage medium, which is then used to heat water to feed a central heating system and/or a sanitary hot water system. Also sometimes called a dry core storage boiler.

In future, the mandate could be extended to further appliances if new technologies emerge that have the potential to be used flexibly.

28. **Do you agree that the smart mandate should initially apply only to hydronic heat pumps, electric storage heaters and heat batteries? Please explain your answer.**

29. **Do you have a view, and supporting evidence, on which appliances the mandate should be extended to include in the future, and by when?**

30. **Do you have a view, and supporting evidence, on the impact that the proposed mandate may have on different consumer groups, for example low income and vulnerable consumers, in terms of upfront costs, running costs or otherwise? What further action is needed to ensure all groups can benefit from smart heating?**

Definition of a smart heating appliance

For the purpose of the smart mandate, the following definition is proposed, in line with how Government defines an ESA:

Smart electric heating appliance: An electric heating appliance which is communications-enabled and capable responding automatically to incentive signals (such as price) and/or other more direct control signals by shifting or modulating its electricity consumption.

Government recognises there may be different approaches to delivering smart functionality in practice and does not intend to specify how it is delivered, provided it meets the required outcomes. As such, Government expects that energy smart functionality could be achieved either through embedded connectivity, or with an add-on module to enable communication and control.

31. **Do you agree with the proposed definition and approach to delivering smart functionality for electric heating appliances? Please explain your answer. If proposing additional requirements to include in the definition, please provide evidence on the costs and benefits of such requirements.**

Timing of implementation

Government is seeking enabling powers in the Energy Security Bill to require minimum levels of smart functionality for electric heating appliances and intends to implement the smart mandate for the initial cohort of devices proposed above in 2025 through secondary legislation. This would see a phased introduction of requirements for heating appliances, with the smart mandate introduced ahead of the proposals set out in the 'ESA Standards' section of Chapter 4 – similar to the phased approach that has been taken for electric vehicle charge points. Heat pump deployment is scaling up rapidly and we want to ensure that heat pumps, storage heaters and heat batteries are being installed as smart from the outset to maximise the benefits they offer. Given the long lifetime of heating appliances, e.g., 15 to 20 years for heat pumps, mandating smart functionality from 2025 will future proof installations, and ensure that appliances installed in this decade are able to support and participate in a smart and flexible energy system. Implementing in 2025 will also align with the introduction of the Future Homes Standard and the Future Buildings Standard, ensuring that the projected 200,000 heat pumps that we expect to see installed annually in new build domestic properties will be able to operate smartly, eliminating further costs and disruption which can be associated with retrofit.

This target date also aligns with the end of the four-year smart meter Targets Framework and the introduction of a market-wide half hourly settlement in 2025, meaning more consumers will be able to use tariffs which underpin the benefits provided by smart electric heating appliances.

Government laid regulations in December 2021 to mandate that private electric vehicle charge points should have smart functionality, which will come into force this year. Many heat pumps already in the market already have smart functionality too and, although smart functionality for

storage heaters and heat batteries may not be as well established, we do not expect the regulations to require a significant step change from industry to meet this timeframe.

32. Do you agree with the proposal to implement the smart heating mandate from 2025? Please explain your answer.

Longer term approach

Maximising the potential of the smart functionality of a heating appliance – particularly a heat pump – can be dependent on the thermal performance of a building's fabric, the heat emitters in a building, and the amount of thermal storage available. The more thermal storage and/or the greater levels of energy efficiency a building has, the longer the duration that a heat pump can be switched off or modulated down to provide flexibility, without negatively impacting on the comfort of the building occupants.

33. Do you have a view on what other measures could be taken, in addition to the proposals in this consultation, to ensure heat pumps can provide this flexibility, for example a minimum level of thermal storage?

Extension of a 'smart mandate' to other devices

Government has already established a regulatory framework to require all private electric vehicle charge points to have smart functionality and the proposals set out in this consultation would build on this and develop a similar smart 'mandate' for a wide range of electric heating appliances. However, we would also welcome views on whether there are any other consumer appliances that we should consider introducing minimum 'smart functionality' requirements for, such as home batteries.

34. Should Government consider introducing a 'smart mandate' for domestic-scale battery systems or any other appliances? If so, what appliances and why?

7. Regulation of Organisations

This chapter proposes introducing regulatory requirements on organisations providing Demand Supply Response (DSR) to domestic and small non-domestic consumers. It includes proposals to use a flexible and proportionate licensing framework as the regulatory approach, developed to meet design principles relating to proportionality, scalability, and digital-by-design, amongst others. It seeks views on the specific aims of future requirements, relating to consumer protection, data privacy, interoperability, grid stability and cyber security.

To unlock the benefits of DSR for consumers and the energy system, we not only need to put in the right technical frameworks to enable DSR, but we also need to give consumers confidence to participate. We need to ensure that these organisations providing DSR act in a way which not only supports their own business objectives, but which also benefits the energy system as well as consumers.

Existing regulation, such as general-purpose consumer protection law, provides some support for domestic and small non-domestic consumers. We have also seen voluntary solutions emerge, such as standards and codes of conduct.[61] However, as DSR uptake grows, we expect more formal requirements on organisations to be needed. This will not only benefit consumers but also help protect the reputation of the DSR sector and give responsible organisations confidence that they are not being undercut by poor business practices.

Overarching Approach

Government intends to establish a proportionate and flexible regulatory framework for organisations providing DSR to domestic and small non-domestic consumers. Government's view is that this could bring several benefits, to consumers, industry, and the energy system.

- **For consumers**: it would improve trust and confidence in DSR, ensuring consumers know they can rely on a minimum standard of service. This would help consumers access new services that reduce costs and provide new sources of revenue.
- **For industry**: it would develop a competitive market with a 'level playing field' between organisations. Greater consumer confidence in DSR will also help the market to grow.
- **For the energy system**: it would improve the ability to monitor and mitigate risks to grid stability, reducing costs of managing the energy system for all.

Government's view is that licensing, if developed and implemented appropriately, can accommodate a wide range of different actors and activities, and can be implemented in a way that is proportionate to the risks posed by different organisations.

[61] Such as Flex Assure: https://www.flexassure.org/ viewed 9 May 2022

Existing licensing frameworks in the energy sector provide some level of precedent and are relevant to considering future scheme design. However, Government's expectation is that licensing for DSR is likely to be substantially different from existing energy system licences. A licensing framework for DSR would be required to accommodate the diversity and differing risk profiles of future licensees, whilst preserving innovation and enabling sector growth.

Government is seeking enabling powers in the Energy Security Bill to extend the existing regulatory scheme for licensing within the energy sector, to allow it to make activities associated with load control into licensable activities. We propose to use these powers to establish a proportionate and flexible licensing framework for organisations providing DSR to domestic and small non-domestic consumers. This framework would be regulated by Ofgem, extending their current duties as the regulator for the British energy sector.

Organisations in Scope

Government proposes in the first instance to focus licensing on activities associated with the provision of demand-side response to domestic and small non-domestic consumers. This intends to ensure consumers have the confidence to use their appliances for DSR, unlocking the benefits that flexibility can provide. More specifically, we propose that future regulation should focus on activities relating to:

- remote load control of appliances for the purposes of DSR, and
- entering into arrangements with domestic and small non-domestic consumers for the purposes of DSR.

We are currently considering including all approaches to DSR services (including optimisation against time-of-use tariffs) and provision of DSR for all types of appliances used by domestic or small non-domestic consumers. Our intent is to ensure all risks associated to the provision of DSR can be mitigated proportionately, effectively, and evenly.

For the avoidance of doubt, Government is not considering licensing any form of automated load control unrelated to DSR. For instance, smart Home Assistants that facilitate home automation, or operators of other internet-of-things products. This is because these types of control are personal consumer choices, rather than designed to deliver wider energy system benefits.

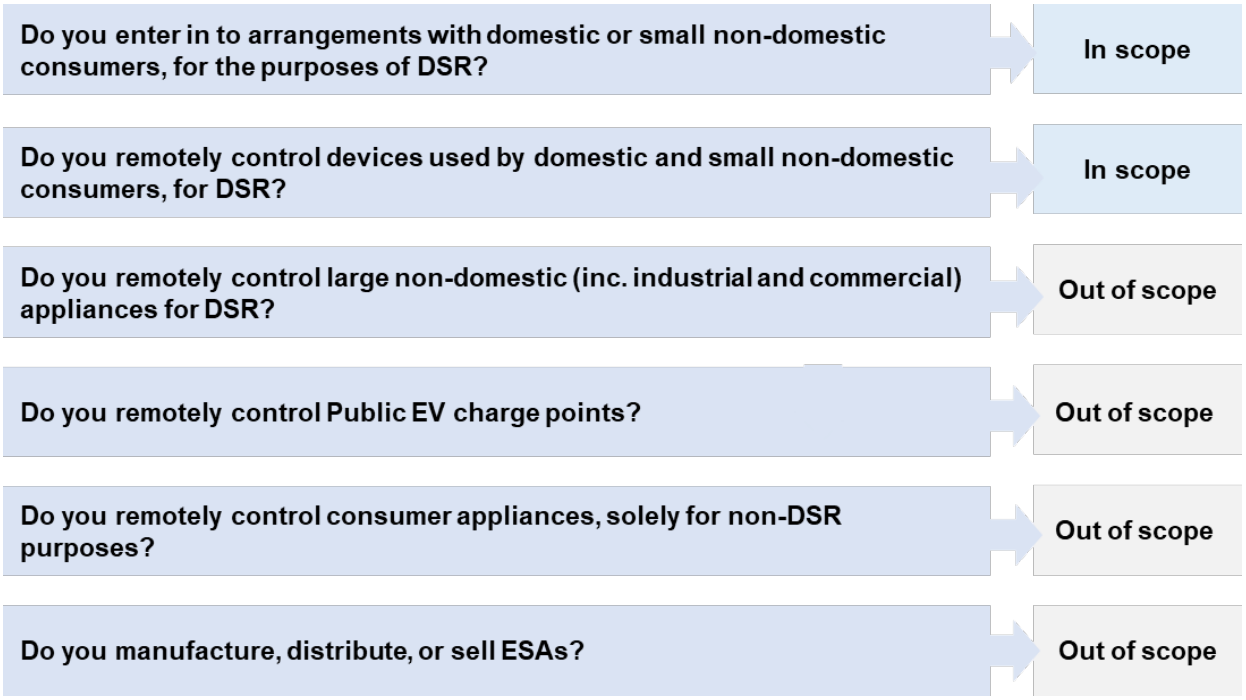
At this stage, we do not propose licensing organisations providing DSR to larger industrial and commercial consumers, given existing mechanisms in place to mitigate risks. We also intend to exclude EV public charge point operators, recognising the differences in this sector compared to our intended scope. However, we will keep this position under review.

Government, in consultation with Ofgem, will need to define the exact scope of activities captured by the new licensing framework in secondary legislation. There are different potential approaches we could take, and these will need to be considered further in consultation with industry. For instance, we could establish the scope of regulations with reference to type of consumer (i.e. domestic or small non-domestic), and/or the type of ESA (such as private EV

charge points, heat pumps, and other ESAs covered by the proposals set out in earlier chapters in this consultation).

Figure 2, below, gives an illustration of organisations which would fall into the scope in the first instance. We would welcome initial views on the most suitable approach.

Figure 2: Proposed scope of future licenses



35. **Do you agree that licensing should initially focus on organisations providing DSR for domestic and small non-domestic consumers? Should there be any exemptions to these requirements? If so, why?**

36. **Do you have initial views on how a licensing scheme should be implemented – for instance, should it be linked to providers of services relating to specific products, linked to the size of the consumer, or some other approach?**

Design Principles

As is stated above, Government expects that the future regulatory framework for licensing could be very different to how existing licences in the energy sector work today. We propose that design of this framework should be informed by several principles, such as:

- **Scalable and proportionate** – regulatory requirements and other aspects of the framework should be suitable for organisations with different sizes and risks posed.
- **Proactive** – organisations should proactively share data with the regulator to support compliance.
- **Evidence driven** – requirements should be grounded in evidence that illustrates what risks must be mitigated.

- **Digital-by-design** – all processes required should be delivered via digital means, such as submission of applications for licences and notification of approval electronically.[62]
- **Support market access and enable innovation** – unnecessary barriers to new entrants obtaining a licence should be avoided.

We believe these principles will need to be a guide to development but not a constraint on future design.

37. What design principles do you agree or disagree with? What principles would you like to be added?

Proportionality

Government recognises that organisational requirements need to be proportionate, to ensure that organisations are not subject to unreasonable barriers to entry or operation in the sector, and incentives to innovation are maintained. This is also recognised in the better regulation framework.[63] Government intends to consider whether licence conditions could be universal to all participants or scaled depending on the size of the organisation's DSR activities and level of risk that it presents. For instance:

- Licensing could be lighter touch for smaller new entrants, similar to the style of general authorisation regimes that have been used within the telecommunications sector, whereby firms register with Ofcom and agree to abide to general requirements.
- For larger organisations who would present more risk to grid stability and consumer protection, a more comprehensive set of licence requirements may be needed to set out specific regulatory requirements.

38. How should proportionality be delivered in a future licensing framework?

Proposed Contents of Licences

Through this consultation, we want to engage with industry and stakeholders from the outset in designing our future licensing framework. However, we recognise that detailed requirements will take time to develop and will need to be the subject of further consultation. Licensing requirements will also need to be developed alongside wider regulatory measures set out in this consultation. At this stage, we are keen to gather views on areas that organisational requirements should cover, and potential requirements that could be included. Our initial proposals are set out below.

[62] Energy Systems Catapult (2022) Digitalising Licensing in Energy, https://es.catapult.org.uk/report/digitalising-licensing-in-energy/ sets out an approach for digitalised licensing
[63] BEIS (2018) Better regulation framework, https://www.gov.uk/government/publications/better-regulation-framework

Consumer Protection and Data Privacy

The existing electricity supply licence conditions provide protections for consumers entering into contracts/agreements with energy suppliers. However, there are no such specific protections, outside of existing consumer protection law, for consumers entering into agreements with organisations providing DSR. As DSR becomes more popular and organisations remotely control greater volumes of domestic electricity load, the risk of consumer harm could increase. Furthermore, lack of consumer confidence could hinder uptake.

We are considering specific areas where additional protection may be required including:

- A consumer's ability to compare service offerings, specifications, or charges – for instance, ensuring information around offers is provided in a standardised way.
- A consumer's ability to make informed choices – for instance, to provide information and advice on whether product/service is appropriate for a consumer.
- Ensuring consumers are not unfairly 'locked-in' to certain services or 'locked-out' from better propositions through practices of organisations – for instance, protecting against unreasonable terms and conditions.
- Ensure organisations are not able to use their privileged control of consumer devices to cause detriment to consumers – for instance, ensuring organisations control ESAs in a way which delivers consumer preferences and choices.
- Additional support for vulnerable consumers – for instance, considering what additional requirements may be necessary to help to enable low income and vulnerable consumers to participate in a smart energy system.[64]
- Routes to redress – for instance, the need for an ombudsman to independently handle disputes between consumers and organisations, setting possible appropriate compensation.
- Managing risks around insolvency of organisations – for instance, to ensure a consumer isn't left without a usable device or service which has been paid for.

Consumer data privacy protections are also important for ensuring confidence in the sector as new products and services emerge. We will consider whether frameworks for data privacy could be required for DSR beyond the protections already provided in the General Data Protection Regulation, as is seen in areas such as Smart Metering.[65]

39. What additional protections for consumers could be required from a future licensing framework beyond those contained in existing consumer protection law?

[64] BEIS (2021), How can innovation deliver a smart energy system that works for low income and vulnerable consumers?, https://www.gov.uk/Government/publications/participation-of-low-income-and-vulnerable-consumers-in-a-smart-energy-system

[65] BEIS (2018), Review of smart metering data access and privacy framework, https://www.gov.uk/Government/publications/smart-metering-implementation-programme-review-of-the-data-access-and-privacy-framework

40. Are additional data privacy protections required for DSR beyond those existing in law through the General Data Protection Regulation? If so, what additional measures should be introduced and why?

Cyber Security

This consultation includes a number of proposals that will impact on the cyber security of organisations which provide DSR. We do not intend on duplicating these protections in any future licensing regime. However, there may be organisations that are out of scope of those regulations, where there are still benefits of ensuring a certain level of cyber security protections are in place – for example, there may be organisations that fall below the thresholds proposed for inclusion in the Network and Information Systems (NIS)[66] regulations but where cyber-attacks could still cause consumer detriment and undermine confidence in energy smart appliances (ESAs).

In light of this, we may need to introduce additional requirements on organisations in order to protect consumers from risks (such as data loss or misuse of ESAs), and to mitigate against risk of more localised disruption to energy system. If we were to implement further cyber security measures, we would ensure they are compatible with the proposals in this consultation to apply the NIS regulations to the largest load controllers (see Chapter 2), and propose considering the following four areas, drawn from the Cyber Assessment Framework:[67]

- **Managing security risk:** Ensuring there are appropriate organisational structures, policies, and processes are in place to understand, assess and systematically manage security risks.
- **Protecting against cyber-attack**: Ensuring proportionate security measures are in place to protect licensees from cyber-attack.
- **Detecting cyber security events:** Ensure licensees have appropriate capabilities to ensure security defences remain effective and to detect cyber security events affecting, or with the potential to affect them.
- **Minimising the impact of cyber security incidents**: Ensuring licensees have the capabilities to minimise the adverse impact of a cyber security incident on the operation of essential functions, including the restoration of those functions where necessary.

Government welcomes views on what cyber security requirements could be needed in the future that may not be covered by proposals elsewhere in this consultation.

41. Do you think that licensing requirements could be appropriate to manage cyber security risk in future, alongside the device level and (for the largest load controllers) NIS measures outlined elsewhere in this consultation? Please explain your answer.

[66] DCMS (2018) The NIS Regulations, https://www.gov.uk/government/collections/nis-directive-and-nis-regulations-2018#:~:text=The%20NIS%20Regulations%20provides%20legal,)%20and%20essential%20services%20(transport%2C

[67] NCSC: Cyber Assessment Framework, https://www.ncsc.gov.uk/collection/caf/cyber-assessment-framework

Interoperability

Earlier chapters of this consultation establish the technical frameworks to deliver interoperability of ESAs and we do not expect extensive licence conditions will need to be placed on DSR Service Providers (DSRSPs) on the technical elements of interoperability. However, there are risks that DSRSPs could use their market position to unfairly lock consumers into particular services or tariffs. We therefore anticipate that licence conditions may need to be introduced to deliver the following high-level outcomes:

- Ensure DSRSPs operate systems in a way that avoids barriers to switching
- Ensures contracts don't unfairly lock consumers in
- Ensure that DSRSP registration/deregistration of appliances does not compromise the appliance or consumer experience.

42. Do you agree that licences should contain conditions to ensure that organisations are not able to use their market position to hinder consumer switching or undermine delivery of Government's objectives for interoperable energy smart appliances?

Grid Stability

It is important that organisations take steps to avoid inadvertently compromising grid stability. For example, while device-level requirements can help individual devices mitigate grid stability risks, there may also be benefits in placing requirements on organisations to ensure that they appropriately manage their portfolios of devices in aggregate, for instance by staggering changes in load in certain scenarios or avoiding synchronous software updates. We are also considering whether requirements may be beneficial to grid stability in other areas too, such as requiring organisations to consider local network capacity when synchronising their managed appliances, and to engage with DNOs to inform them of amounts of load they control.

43. Do you agree that licence conditions may be a useful tool to help mitigate risks to grid stability alongside the measures outlined elsewhere in this consultation? What licence conditions may be necessary to achieve this?

Implementation

We recognise that developing the detail of our future licensing proposals will take time and our aim is to start introducing requirements from the mid-2020s. This timeframe intends to provide protections and establish good practice whilst the sector is still growing. Our aim is to ensure that the most pressing risks are mitigated before they can materialise and potentially damage consumer confidence in DSR, given the important role it will play in decarbonising our electricity system as part of the transition to net zero.

8. Next steps

Government anticipates implementing these proposals over a period of several years, recognising the different costs, benefits, and complexities of different proposal. For example, we expect our proposals to make time-of-use tariff data openly available, could be implemented sooner. However, other measures are likely to take longer. For instance, we propose establishing a licensing framework, introducing minimum requirements relating to smart heating, and extending larger load controllers to the provisions of the NIS Regulation by the mid-2020s.

Timescales for implementing our proposals for ESA standards are subject to the most uncertainty, due to the complexity of potentially establishing common systems for ESAs and the need to establish long-term governance arrangements. In addition to the above, availability of parliamentary time will also impact when we can introduce the legislation required to implement these proposals.

Whilst Government recognises the desire for industry and consumers to have certainty on implementation timings across our proposals now, setting more specific timeframes without further engagement will be counterproductive to our policy objectives. We aim to provide further clarity in the future following engagement with affected parties, alongside further consultation on specific proposals. We are also clear that prior to implementation, our proposals will need to be subjected to full impact assessments to ensure that any costs imposed are proportionate to the benefits. To inform analysis of proposals and future work, we have published an analytical annex separately from this consultation. This sets out a series of questions that aim to inform our understanding on the impacts of our proposals, as well as to inform future consultations and impact assessments.

We are conscious of the need to balance certainty with transparency and engagement. This consultation has aimed to do that by setting a clear direction of travel and seeking views on that. Respondents will have up to 12 weeks to respond, with our final deadline for responses being 28th September 2022. We will aim to publish a Government response this winter including, subject to the outcome of the consultation, more detailed plans on next steps for implementation.

44. Are there other risks to grid stability or cyber security from other forms of load control that are not covered by the proposals in this consultation? If so, how significant are these and how should they be mitigated?

Consultation questions

1. What are your views on the over-arching timings of implementation of these proposals, including the proposed approach to phasing?

2. Do you agree with the Government's proposal to make certain load controllers subject to the obligations in the NIS Regulations? Please explain your answer.

3. Do you agree with the Government's proposal of setting a threshold requirement of 300MW of remote load control for a load controller to be considered an operator of an essential service under the NIS Regulations? Please explain your answer, and provide supporting evidence.

4. Are there any other threshold metrics that should be considered, for instance if organisations have more than a certain number of customers/appliances connected?

5. Do you agree with the Government's proposal of using the Cyber Assessment Framework (CAF) to support the implementation of the NIS requirements for load controllers? Please explain your answer.

6. Do you agree with our proposed outcomes for interoperability? Please explain your answer.

7. What are your views on the initial proposed outcomes for cyber security of Energy Smart Appliances? Is there anything missing or not relevant?

8. Do you agree with Government's proposed data privacy outcomes for ESAs?

9. Do you agree with the risks to grid stability and proposed outcomes Government has identified? Is there anything missing or not relevant?

10. Do you agree with Government's proposals to make time-of-use tariff data openly available in a common format for Energy Smart Appliances?

11. Do you agree that the Smart Energy Code could provide the appropriate governance for development of common data standards? Please explain your answer.

12. How should Government ensure that Energy Smart Appliances integrate with time-of-use tariffs, beyond providing interoperability with tariff data?

13. Should government consider standardisation of other types of 'incentive data' used by ESAs for DSR? Please consider what types of data and how they could be standardised.

14. Do you agree that Government should establish regulatory requirements to promote adoption of ESA standards, and what would be your preferred approach? Please consider the advantages and disadvantages of an 'approved standards' (Option 1) vs. 'mandated' (Option 2) approach.

15. Do you agree that a standard based on PAS 1878 should be used in the future regulation of ESAs?

16. Do you agree that Government proposals for ESA standards should apply to domestic-scale ESAs with the highest potential for flexibility, including private EV charge points, batteries, heat pumps, storage heaters and heat batteries? Please consider whether any other types of ESA should be in scope.

17. What is your preferred option for developing and maintaining ESA standards in the future? Are there other options we should be considering? Please explain how you would expect your preferred option working in practice.

18. Should Government mandate a randomised delay for ESAs, including heat pumps, storage heaters, heat batteries and batteries, to mitigate against risks to grid stability, in advance of longer-term ESA standards? Views are welcome on how a randomised delay could operate and on alternative mitigations.

19. Should minimum device-level cyber security requirements be implemented for heat pumps, storage heaters, heat batteries and batteries, prior to implementation of enduring ESA standards? Should any other ESAs be considered?

20. Is ETSI 303 645 an appropriate standard for minimum device-level cyber security requirements for ESAs?

21. Do you agree that common systems could be required to mitigate system-wide risks? What issues will need to be considered in the design of such systems?

22. What issues will Government need to consider when reaching a decision on delivery approach for common systems?

23. What are the key considerations for design of governance during the development, transition and delivery phases of implementation?

24. Are there any considerations Government has not mentioned above that should be factored into future policy on assurance? Please consider assurance for devices and associated systems, such as ‘cloud’ platforms.

25. What is your preferred approach for assurance for ESAs, and why? Please provide any evidence on the relative impacts, costs, and benefits of different approaches.

26. Do you think a labelling scheme for ESAs could help promote consumer uptake in DSR from ESAs? If yes, what type and form of labelling would be most beneficial?

27. What factors should government take account of when considering how the costs of delivering these arrangements should be distributed and recovered?

28. Do you agree that the smart mandate should initially apply only to hydronic heat pumps, electric storage heaters and heat batteries? Please explain your answer.

29. Do you have a view, and supporting evidence, on which appliances the mandate should be extended to include in the future, and by when?

30. Do you have a view, and supporting evidence, on the impact that the proposed mandate may have on different consumer groups, for example low income and vulnerable consumers, in terms of upfront costs, running costs or otherwise? What further action is needed to ensure all groups can benefit from smart heating?

31. Do you agree with the proposed definition and approach to delivering smart functionality for electric heating appliances? Please explain your answer. If proposing additional requirements to include in the definition, please provide evidence on the costs and benefits of such requirements.

32. Do you agree with the proposal to implement the smart heating mandate from 2025? Please explain your answer.

33. Do you have a view on what other measures could be taken, in addition to the proposals in this consultation, to ensure heat pumps can provide this flexibility, for example a minimum level of thermal storage?

34. Should Government consider introducing a ‘smart mandate’ for domestic-scale battery systems or any other appliances? If so, what appliances and why?

35. Do you agree that licensing should initially focus on organisations providing DSR for domestic and small non-domestic consumers? Should there be any exemptions to these requirements? If so, why?

36. Do you have initial views on how a licensing scheme should be implemented – for instance, should it be linked to providers of services relating to specific products, linked to the size of the consumer, or some other approach?

37. What design principles do you agree or disagree with? What principles would you like to be added?

38. How should proportionality be delivered in a future licensing framework?

39. What additional protections for consumers could be required from a future licensing framework beyond those contained in existing consumer protection law?

40. Are additional data privacy protections required for DSR beyond those existing in law through the General Data Protection Regulation? If so, what additional measures should be introduced and why?

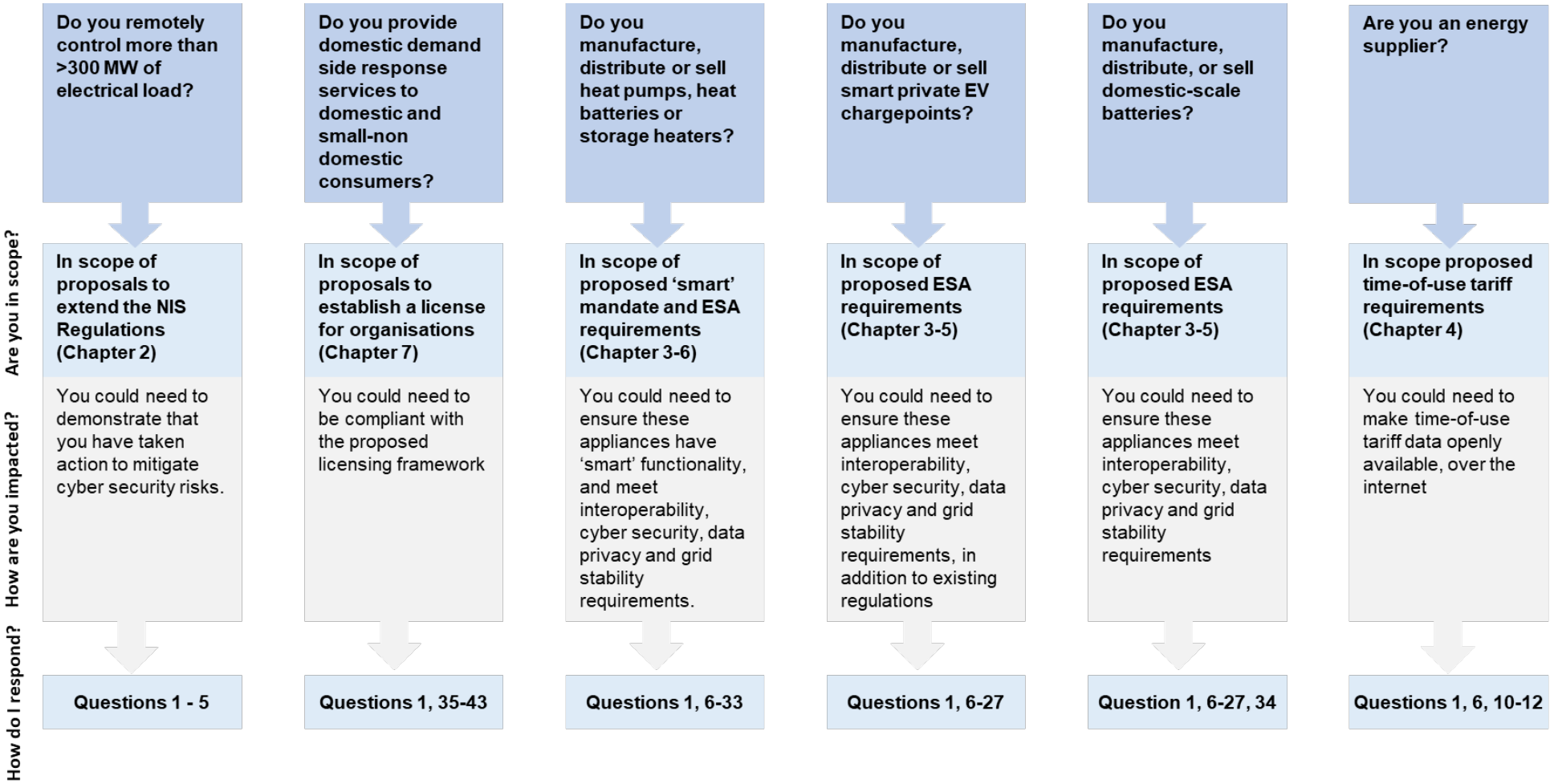
41. Do you think that licensing requirements could be appropriate to manage cyber security risk in future, alongside the device level and (for the largest load controllers) NIS measures outlined elsewhere in this consultation? Please explain your answer.

42. Do you agree that licences should contain conditions to ensure that organisations are not able to use their market position to hinder consumer switching or undermine delivery of Government’s objectives for interoperable energy smart appliances?

43. Do you agree that licence conditions may be a useful tool to help mitigate risks to grid stability alongside the measures outlined elsewhere in this consultation? What licence conditions may be necessary to achieve this?

44. Are there other risks to grid stability or cyber security from other forms of load control that are not covered by the proposals in this consultation? If so, how significant are these and how should they be mitigated?

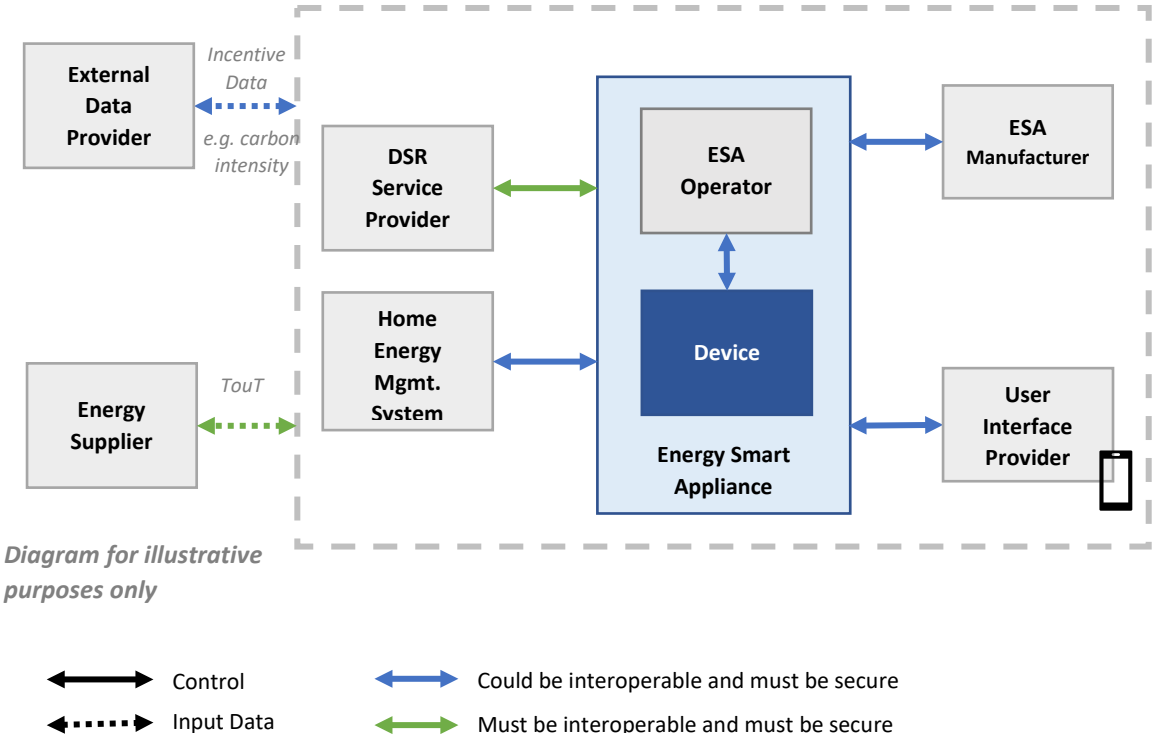
Appendix 1: Summary of impacts



Appendix 2: ESA System Overview

Figure 3, below, depicts the overall system and different functions and roles needed to deliver the types of DSR through ESAs, as well as a glossary of terms for each of these functions and roles.

Figure 3: The system for delivering DSR through ESAs



Energy smart appliances are consumer devices that are communications-enabled and able to respond automatically to price and/or other signals by shifting or modulating energy consumption and/or energy production. They typically consist of a physical, tangible **appliance**, which can be controlled manually by the consumer, or remotely through an **ESA Operator's** systems.

The **ESA Manufacturer** is responsible for the security and safety of the ESA, and for providing ongoing firmware or security upgrades.

The **User Interface Provider** provides the consumer 'app' that allows the consumer to remotely control their appliance and input their consumer preference – often a smart phone app.

The **DSR Service Provider** can control or configure the ESA's energy usage or production, in order to provide a service to organisations responsible for the transmission, distribution, supply or balancing of energy. This is with the consumer's consent and within the constraint of consumer preferences. The consumer is often rewarded for having a DSR Service Provider, such as through a discounted tariff from their energy supplier, or direct remuneration.

The **ESA Operator** provides the systems and connectivity to enable remote control or configuration of ESAs by consumers. In the context of EV charge points, these organisations are often referred to as ‘charge point operators. In today’s market, this is typically via a remote, cloud-based operating system.

The **Home Energy Management System (HEMS)** can control of configure the ESA’s energy usage or production, in order to optimise usage against other appliances in the premises, such as a solar panel or other ESAs. Optionally, a HEMS can be an ESA in its own right, offering flexibility services to the DSR Service Provider through controlling the appliances it connects to.

This **ESA Manufacturer, User Interface Provider, DSR Service Provider** and **HEMS** can all connect directly to the **appliance** or via the **ESA Operator’s** remote systems.

ESAs may use external data to determine how the ESA operates. **Energy suppliers** determine the consumer’s energy retail tariff, include time-of-use tariffs that change the cost of energy based on time of day in 30-minute settlement periods. Other **external data providers** will provide other data used by ESAs, such as carbon intensity.

Appendix 3: Glossary

Term	Definition
Aggregator	An organisation that aggregates the controllable load of electricity consumers to provide a consolidated DSR service.
Anomaly Detection	A mechanism for detecting one or more messages that are intended to be Remotely communicated to one or more devices and that are identified as being anomalous by virtue of either their content or their quantity.
Balancing Mechanism	The mechanism set out in the Balancing and Settlement Code that allows the ESO to adjust the amount of generation from generating units and the amount of electricity consumption by various demands.
Balancing Service	One of a number of services procured by the ESO to help it maintain the frequency, voltage and other needs of the electricity transmission system.
BEIS	The Department for Business, Energy and Industrial Strategy
British Standards Institution (BSI)	The national standards body for the United Kingdom.
Competent Authority	The entities responsible for the oversight and enforcement of the Network and Information Systems (NIS) Regulations 2018. In the energy sector, this means BEIS and GEMA.
Control or Configure (an Energy Smart Appliance)	To change the amount of electricity a device consumes or exports at any given time (either directly or indirectly, through configuration) by means of a Remote communication.
Cyber Assessment Framework (CAF)	the framework of that name established by NCSC to assist in carrying out cyber resilience assessments.
Dynamic Time of Use Tariff	A Time of Use Tariff under which the prices applicable to various time periods themselves change over the term of the tariff.
Data Communications Company (DCC)	The company that communicates with Smart Meters in GB on behalf of energy suppliers and other parties.
Demand Side Response (DSR)	Load Control to help meet the needs of the energy system, typically to benefit the transmission network, distribution network, or another third party delivered by a Demand Side Response Service or Optimisation
Demand Side Response Service	The use of Load Control to provide a Service to help manage the Transmission or Distribution Network.
Demand Side Response Service Provider .	An organisation which provides a Demand Side Response Service. Also DSR Service Provider or DSRSP.
Demand Side Response Service Provider Interoperability	In relation to an ESA, that the identity of any DSR Service Provider that is authorised to control or configure the device may be changed easily and without the need for a service provider visit to the ESA
Distribution Network / Distribution Network Operator (DNO)	A network or the operator of a network that is authorised to be operated by the holder of an electricity distribution licence.
Elexon	The company that administers and provides central services under the Balancing and Settlement Code.

Energy Smart Appliance (ESA)	a device which is communications-enabled and capable of responding automatically to price and/or other signals by shifting or modulating its electricity consumption and/or production.
Electricity System Operator (ESO)	The organisation that operates the GB electricity transmission system.
Flexibility Innovation Programme	An UK Government programme, part of BEIS's Net Zero Innovation Portfolio, that looks to support innovative solutions to enable large-scale widespread electricity system flexibility.
Flexibility Service Provider	Another term for a DSR service provider
Gas and Electricity Markets Authority (GEMA)	The energy regulator for GB.
Home Energy Management System (HEMS)	A device or system used to control one or more ESAs within a consumer premises.
IDSR	One of a number of initiatives with BEIS's Flexibility Innovation Programme to trial the interoperable provision of DSR services from energy smart appliances.
Interoperability	The ability of a product or system to operate in conjunction with other products and systems
Load Control	The activity of configuring or controlling the consumption, discharge or production of electricity of devices.
Load Controller	A person carrying out Load Control.
Local Area Network	A communications network that is confined to a moderate geographical area.
National Cyber Security Centre (NCSC)	The organisation of that name established by the UK Government to, amongst other things, provide advice in relation to cyber security.
Network and Information Systems (NIS) Regulations	The Network and Information Systems Regulations 2018, that require organisations to meet specified cyber security requirements.
Non-DSR Load Control	Load Control for purposes unrelated to the provision of DSR.
Ofgem	The Office of Gas and Electricity Markets, i.e. the organisation supporting the Gas and Electricity Markets Authority.
Operator of Essential Services (OES)	A person to whom the NIS Regulations apply.
Optimisation	In relation to DSR, delivering a requested output (e.g. EV range, home temperature, etc.) whilst minimising or maximising other factors such as cost, carbon intensity, microgeneration etc.
PAS 1878	The Publicly Available Specification published by BSI specifying requirements and criteria that an electrical appliance needs to meet in order to perform and be classified as an ESA.
PAS 1879	The Publicly Available Specification published by BSI setting out a common definition of DSR services for actors operating within the consumer energy supply chain and providing recommendations to support the operation of ESAs.
Personal Tariff Data	Information that identifies the energy tariff of an individual energy consumer

Public Key Infrastructure	A system for managing cryptographic material that is used to secure and encrypt communications.
Public Tariff Data	Information that identifies one or more tariffs offered by one or more energy suppliers.
Radio Teleswitch Service (RTS)	The radio service used to switch certain electricity meters between different tariff rates.
RECCo	The company that procures central services under the Retail Energy Code.
Remote	means in relation to a communication, that is conveyed (at least in part) over a Wide Area Electronic Communications Network.
Retail Energy Code (REC)	A central industry document that sets out how centralised information is managed including, for example, which energy supplier supplies which consumer.
Smart Energy Code (SEC)	A central industry document that sets out how energy suppliers and other parties communicate with Smart Meters via the DCC.
Smart Energy Code Administrator and Secretariat (SECAS)	A company that provides administration services under the SEC.
Single Rate Tariff	A tariff under which the unit price does not vary depending on when energy is consumed or produced, for the term of the Tariff
Smart	means, in relation to a device, the ability of the device to respond in real time to remote communication signals, using digital technologies, to deliver a service.
Smart Tariff	a tariff where the cost of energy changes based one or more factors such as time, quantity of energy consumed or produced, or the appliance it is used by etc.
Static Time of Use Tariff	A Time of Use Tariff under which the prices applicable to various time periods are fixed, forthe term of the Tariff.
Technical standard	A standard that specifies technical requirements for devices.
Tariff	The charges applied to a consumer for their energy supply (and the associated contract terms)
Tariff Interoperability	In relation to an ESA, the ability of an ESA to be used with a tariff from any energy supplier, easily and without a service provider visit to the ESA
Time of use Tariff (TOUT)	An electricity Tariff under which the unit price for electricity varies throughout the day.
Transmission Network	The high voltage system for the transmission of electricity in GB.
Wide-Area Network (WAN)	A wide ranging electronic communications network (as distinct from a local area network or a personal area network).

This consultation is available from: www.gov.uk/government/consultations/delivering-a-smart-and-secure-electricity-system-the-interoperability-and-cyber-security-of-energy-smart-appliances-and-remote-load-control

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