Department for
Business, Energy
& Industrial Strategy

Delivering a smart and secure electricity system

Analytical annex

July 2022

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

Contents

About this document

This annex aims to present and gather evidence on the main proposals in the 2022 consultation on delivering a smart and secure electricity system. At the point of consulting on secondary legislation and other measures, impact assessments will accompany those more detailed proposals.

This annex is structured as follows:

- **Section one** reaffirms the strategic case for increased system flexibility from Demand Side Response (DSR).
- **Section two** sets out the case for government intervention.
- **Section three** provides a high-level identification and assessment of potential impacts of our consultation proposals to different stakeholder groups.
- **Section four** asks questions to help strengthen our evidence base.

Section 1: The strategic case for increased system flexibility from DSR

Overview of government's objectives

A secure, smart, flexible energy system is critical to support energy system independence and ensure net zero is achieved at least cost by 2050. The 2021 Smart Systems and Flexibility Plan (SSFP) sets out how system flexibility will become increasingly important as electricity demand rises due to the electrification of transport, heat and industrial processes, and we integrate intermittent renewables, such as solar and wind, into our power supply.

Flexibility will help reduce the amount of generation and network capacity needed to address this additional demand and meet net zero targets. Analysis in the SSFP estimates that these cost reductions could be up to £10 billion per year in 2050[1]. This, in turn, will reduce costs for all electricity consumers.

To date, much of the flexibility that balances and provides stability to our system has been provided by fossil fuels, as we turn up or turn down coal or gas fired power stations. In the future, we need an energy system that matches new sources of demand to renewable generation – both nationally and locally – by using low carbon flexibility across the system.

Low carbon flexibility can be provided by different technologies such as electricity storage (e.g. batteries) and flexible generation assets (e.g. interconnectors). DSR is a form of flexibility whereby consumers change when they use or produce energy to reduce the impact on the energy system. Smart appliances, such as smart electric vehicle (EV) charge points and smart heating appliances, can provide DSR in different ways, such as responding to a time-of-use (ToU) tariff[2] or providing a contracted DSR service.

However, there are risks to the future growth of this sector. Not all tariffs and services can be used with all devices, furthermore, there are limited consumer protections to build confidence in the market. In addition to this, there are cyber security related risks as widespread use of connected appliances[3], such as energy smart appliances, which could increase the potential for cyber-attack. These risks could lead to consumer detriment or wider energy system disruption.

The proposals set out in the consultation intend to enable the scale-up of competitive markets for DSR and energy smart appliances by ensuring consumers have confidence in these products and services, whilst also mitigating risks to the energy system from their uptake. The consultation proposes the overarching regulatory framework for technologies and services that will enable greater DSR uptake.

[1] C. £12bn in 2020 prices. BEIS (2021), Smart systems and flexibility plan 2021: Appendix I – Electricity system flexibility modelling, p. 5.
[2] A time of use tariff is a tariff under which the unit price for electricity varies throughout the day.
[3] 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)

Benefits of Demand Side Response

Demand Side Response is a key form of flexibility and could deliver the following benefits:

1. **Reducing the overall cost of energy to all consumers.** Whilst the scale of future DSR uptake is dependent on several factors, current BEIS evidence suggests DSR could reduce peak demand by 15GW by 2050 in a high flexibility scenario[4], equivalent to approximately 7-10% of the system peak. DSR is part of the potential £10bn per year saving to the energy system. Achieving this potential saving should reduce the overall cost of energy to all consumers, as lower system costs feed through into lower consumer prices.
2. **Enabling the power sector to decarbonise more cost effectively**, through shifting electricity demand to times where low-carbon electricity is more abundant and reducing dependencies on non-renewable power supply. Evidence from the Smart Systems and Flexibility Plan found the difference between the least flexible scenario and the most flexible scenario is about £10bn per year in 2050, or with low demand, about £6bn per year[5]. This assumes at a 5g/kWh carbon intensity with high demand. This view is shared with other studies, which suggest consumer flexibility is one of the most cost-effective ways of reducing carbon emissions, for example by foregoing the need to build additional generation and network capacity[6]. Similarly, recent modelling by the Carbon Trust and Imperial College London showed that a system that deployed flexibility, but without demand side flexibility, could cost around £5bn more per annum in 2050[7].
3. **Rewarding individual consumers for providing value to the energy system**, through enabling consumers to provide DSR in exchange for financial remuneration, cheaper electricity tariffs or other types of reward. The amount of money a consumer could earn from providing DSR will vary according to their behaviour, market conditions and the exact proposition offered to them. For example, Vehicle to Grid (V2G) technology enables bi-directional charging, allowing EV owners to earn further revenues in flexibility markets. The scale of benefits is likely to vary across consumers depending on their driving and charging patterns, however, Project Sciurus, the largest V2G demonstration project to date, estimates that an EV owner could earn revenues of £725 with V2G[8].

Market Growth Potential

The substantial benefits can be realised if the market for Energy Smart Appliances (ESAs) and DSR is encouraged to grow. Table 1 illustrates the potential growth in the uptake of low carbon technologies over the coming decade as transport and heating sectors decarbonise.

---

[4] BEIS (2021), Smart systems and flexibility plan 2021: Appendix 1 – Electricity system modelling, p.23. This comes from domestic and non-domestic DSR, and primarily from smart charging. This does not include Vehicle to Grid (V2G).
[5] See footnote 4.
[6] Analysis by Frontier Economics. Recosting Energy – Powering for the Future Report (2020), (page 40)
[7] Carbon Trust and Imperial College London (2021), Flexibility in Great Britain, (page 106)
[8] Project Sciurus Trial Insights (2021), https://www.cenex.co.uk/app/uploads/2021/05/Sciurus-Trial-Insights.pdf

Table 1: Growth in low carbon technologies

	Current	2030
Heat pumps[9]	55,000 installed per year	At least 600,000 installed per year by 2028
EVs[10]	500,000 on the road in the UK	Around 10,000,000 on the road in UK
Public EV charge points[11]	30,000	300,000 – 720,000

Today, industrial and commercial consumers are providing around 1GW of DSR to the system, but participation from domestic and smaller non-domestic consumers remains at an early stage[12]. By ensuring these low carbon technologies have 'smart' capabilities we can expect the market for load control services and DSR to grow significantly.

The market for DSR is evolving rapidly with innovation in products and services, mergers, acquisitions and new entrants. We estimate, based on internal analysis, there are approximately 80 firms in the UK market that provide DSR in some form. These firms are a diverse mix of organisations such as aggregators, charge point operators and energy suppliers. A description of these different companies can be found in the table below.

Text box 1 – Examples of range of firms which can provide DSR services

Aggregator/DSR service providers (DSRSPs)– e.g. Flexitricity, Centrica, Engie

An aggregator or DSRSP manages flexible assets (such as batteries or EV charge points) to provide DSR services. These typically benefit organisations responsible for supply, balancing, transmission or distribution of energy.

Home/building energy management service provider – e.g. Hive, Evergreen, Moixa

Organisations who can 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, home temperature etc.) optimised against parameters (such as cost or overall energy usage) for multiple ESAs

ESA operator (or charge point operator) – e.g. Tesla, PodPoint

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

[9] BSRIA (2022), 'Heat pumps market analysis 2021' (https://www.bsria.com/uk/), and Heat and Buildings Strategy (2021).
[10] Taking charge: the EV infrastructure strategy (2022).
[11] Taking charge: the EV infrastructure strategy (2022).
[12] National Grid (2021), Future Energy Scenarios Data Workbook, Sheet FL.9

organisations are often referred to as ‘charge point operators’. In today’s market, this is typically via a remote, cloud-based operating system.

Energy Supplier – e.g. EDF Energy, Octopus, OVO

Many organisations providing DSR to consumers also fulfil other roles. Specifically, energy suppliers may already operate across a range of the above functions. For example, they could assume the role of an aggregator, or intend to perform these functions in future. They may also increasingly offer time-of-use tariffs, enabling consumers to benefit directly from shifting their demand.

There is uncertainty around how the market may grow and how consumers will provide DSR through ESAs, due to the significant pace of innovation and market change. Evidence on this is limited, and this document aims to gather additional information from stakeholders on the potential development of the DSR market.

Section 2: The case for intervention

Left to the market alone, growth in this sector could pose risks to consumers and the energy system, which could in turn prevent it from reaching its potential. Without regulation, several market failures are likely to materialise. Collectively these could undermine the policy objectives described in the consultation, and wider government objectives related to achieving net zero, increasing security of energy supply, and reducing fuel poverty.

Interoperability[13]

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

- **Market power** – A firm with a large market share or cost advantage may deliberately prevent rival firms from being interoperable with its products or services, to sell more products or maintain services over a longer period. Alternatively, firms with market power may develop interoperability solutions that favour their specific business, creating barriers to firms offering innovative approaches. Network effects[14] may lead to this issue growing over time.
- **Coordination failure** – Firms may not have the incentive, capability or mechanisms to effectively co-ordinate to deliver interoperability.
- **Externalities** – The benefits to the energy system and consumers from maximising uptake of flexibility could be greater than the private benefit a firm perceives for investing in DSR, leading to a tendency to underinvest. This may be more prevalent in early markets for DSR services, where there may be little incentive for companies to invest additional time and energy in standardisation of products.

Consumer Protection and Data Privacy

Left unregulated, consumers may be exposed to the mis-selling of services, contractual lock-in or the mishandling of personal data. These are likely to occur due to:

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

[13] Interoperability, refers to the ability for products and services to work together effectively. Interoperability between ESAs, tariffs and DSR service providers will ensure consumers can access a range of different propositions and access benefits for providing DSR.
[14] Network effects here means that the more customers that use a particular interoperability standard the greater the value for that interoperability standard.

- **Misalignment of incentives** - Firms may be exposed to incentives to mis-sell services or contracts, or to mishandle personal data.

Cyber Security and Grid Stability

Without additional regulation, firms may underinvest in cyber security[15] or other measures to address grid stability, which could have significant impact, due to the existence of the following market failures:

- **Externalities** - Firms may not fully capture the wider societal benefits of investing in cyber security or grid stability, as this exceeds their private benefit. This is because grid stability is a public good, where the benefits of security or stability are borne by society as a whole, and network operators in the form of a more stable and lower cost energy system. These benefits are non-rivalrous and non-excludable[16]. Equally, the costs of insecurity or instability are also borne by the system. Therefore firms, have an incentive to free ride[17], as they operate insulated from these benefits/costs which reduces their incentive to invest. Organisations primarily view risks to themselves, and not the system, which creates problems when smaller organisations become connected, creating points of vulnerability in the wider system.

- **Imperfect information** - Firms may not be sufficiently equipped to identify, understand, and implement sufficient cyber security or grid stability solutions as they do not fully understand the risk they present to the wider energy system. In addition, firms subject to cyber-crime may not report or may want to play down the severity of cyber security attacks to avoid potential reputational damage and associated financial impact. The aggregate impact of many load controlling devices optimising across the same time of use tariff could cause greater grid instability. However, individual organisations are unlikely to have the necessary information to be aware of this.

Key proposals

The consultation document sets out a range of proposals that intend to address these market failures. The key proposals are summarised below:

- To require organisations controlling large electrical loads (>300MW) to comply with the provisions of the Network and Information Systems (NIS) Regulations, and to be assured by the Cyber Assessment Framework **(Chapter 2).**

- To require energy suppliers to make time-of-use tariff data openly available in a common format, accessible over the internet **(Chapter 3-5).**

[15] These risks are informed by the academic literature, for example "Economic aspects of national cyber security strategies" by P Brangetto, and a DCMS IA on cyber security for consumer products, with both concluding the same market failures.
[16] Non-rivalry suggests the benefit one energy market participant receives from having a stable grid does not reduce the amount of benefit another can receive from having a stable grid. Non-excludability suggests that all energy market participants receive the benefit of a stable grid.
[17] The free rider problem is the burden on a shared resource that is created by its use or overuse by people who aren't paying their fair share for it or aren't paying anything at all.

- 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 EV charge points **(Chapter 3-5).**
- To require larger domestic-scale ESAs, such as EV charge points, heat pumps, storage heaters and heat batteries, to be interoperable with demand-side response service providers, and to meet further requirements for cyber security, grid stability and data privacy **(Chapter 3-5).**
- To establish comprehensive governance arrangements between government and industry to support implementation of the proposals for ESAs **(Chapter 5).**
- To require electric heating appliances with the greatest flexibility potential, namely heat pumps, storage heaters, and heat batteries, to have 'smart' functionality in order to unlock the benefits of the transition to low-carbon electric heating **(Chapter 6).**
- To establish a proportionate and flexible licensing framework for organisations providing demand side response to domestic and small-non-domestic consumers **(Chapter 7).**

Section 3: Potential impacts of proposals

This section provides an overview of the main potential impacts from the proposals. For each group, we provide a summary of the types of costs and benefits and, where available, quantified estimates. It is intended to help identify the key gaps, to best inform future policy development.

Across all areas, the precise impacts will be driven by the details of the regulatory and technical requirements, which will be set out through further consultation on secondary legislation and informed by evidence gathering. Given the early stage of policy development, it is not possible to estimate the specific scale of costs or benefits incurred by organisations in all cases, without this further detail.

It is also noted that firms may operate across several different roles, and therefore be subject to a range of impacts. In addition, the impacts will be dependent on the size and practices of groups impacted – for example, the costs of meeting new cyber security requirements will depend on how cyber secure that organisation is already.

Table 2: How stakeholder groups are affected by the proposals in each chapter

Group	Cyber Security proposals for protecting the energy system (Ch. 2)	ESAs: Outcomes (Ch. 3)	ESAs: Technical frameworks (Ch. 4)	ESAs: Delivery frameworks (Ch. 5)	Smart Electric Heating (Ch. 6)	Regulation of orgs. (Ch. 7)
ESA manufacturers		✓	✓	✓	✓	
Load controllers[18]	✓			✓		✓
Energy suppliers		✓	✓	✓		
Energy system/ network operators	✓	✓	✓	✓	✓	✓
Government/ Ofgem	✓	✓	✓	✓	✓	✓
Central bodies			✓	✓		
Consumers	✓	✓	✓	✓	✓	✓

[18] See Text box 1 for examples of potential load controllers.

This section concludes by discussing distributional impacts on specific consumer groups.

ESA manufacturers

This group includes organisations who produce energy smart appliances, such as EV charge points, heat pumps and batteries. ESA manufacturers will be impacted by proposals to meet ESA requirements (Chapter 3-5) and participate in governance (Chapter 5). Electric heating appliance manufacturers will also be impacted by the proposed smart mandate (Chapter 6). Some of the impacts they may face, and illustrative examples are:

Costs:

- **Manufacturing**: Ongoing costs from providing additional hardware/software to adhere to regulations.
    - **Smart mandate (Chapter 6):** Manufacturers of heat pumps, heat batteries and storage heaters will need to provide additional hardware/software for these devices to include smart functionality. We estimate that the cost of non-smart heat pumps meeting these proposals to be c.£40 per unit[19], with an upper bound of £100[20]. This cost compares to current overall installed price of an air source heat pump of £7-14,000, and a product lifetime of over 15-years. We have limited evidence on the costs for non-smart heat batteries and storage heaters but expect they would be similar. Products that already meet future 'smart' requirements would not incur additional costs[21].
    - **ESA requirements (Chapter 3-5):** Additional costs could be incurred to meet interoperability, cyber security, grid stability and data privacy requirements, although this will depend on the exact requirements agreed through the ESA standards development process. We expect this unit cost to fall over time via economies of scale and innovation.
- **Transition**: One-off costs of changing manufacturing processes to meet requirements or changing existing systems to meet requirements. These costs include designing, testing and implementing changes required.
- **Familiarisation**: Additional technical, legal and managerial resource to read and understand the requirements.
- **Customer service**: Additional resource needed to provide after sale care, following installation of smart technologies.
- **Governance**: Costs associated with participating in governance arrangements.

[19] This does not include additional development costs, such as developing the firmware, that would also need to be considered.
[20] We have used evidence from smart EV charging points to infer 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 a market review of the current retail price of heat pump smart controls.
[21] BEIS's review of heat pump manufacturers' product sheets and initial engagement with industry suggest that at least 43%-55% of current heat pump sales are already internet connectable (with either embedded connectivity or are currently sold as a bundle with add-on module that enables communication).

- **Compliance**: Costs associated with demonstrating compliance, such as through participating in assurance arrangements or submitting required documentation to a regulator.

Benefits:

- **Increased market size**: Increased consumer confidence and improved reputation of ESA manufacturers is expected to increase demand for ESAs and the potential market for manufacturers to sell to.

- **Reduced product development costs**: Benefits to manufacturers from standardised products or processes, such as avoided costs of developing best-practice or engaging bilaterally with other firms.

- **Increased international trade**: Greater uptake of ESAs and increased innovation will enable domestic ESA manufacturers to develop products with export potential, particularly if international markets seek to follow UK market. In addition, growth in uptake of ESAs will develop mutually beneficial international supply chains.

Load controllers

This group includes organisations who remotely control or configure the electrical load of devices, such as ESA operators and DSR service providers. Load controllers controlling over 300MW of load will be impacted by proposals relating to NIS Regulations (Chapter 2). Organisations who provide DSR to domestic and small-non-domestic consumers will be directly impacted by proposals relating to licensing (Chapter 7), and indirectly impacted by proposals for ESAs to be interoperable with DSRSPs (Chapters 3-5). Some of the impacts they may face, and illustrative examples are:

Costs:

- **Adhering to requirements**: There may be transitory and ongoing costs to firms associated with changing business practices to adhere to new requirements, such as consumer protection or cyber security requirements.

    - **NIS**: This may cover organisational changes, additional security spend and reporting security breaches. Additional spend could include software, hardware, risk profiling, staffing costs, potential outsourcing and training to meet NIS requirements. An example of possible organisational change is recruitment of an in-house cyber security team.

    - **Licensing**: This is highly dependent on requirements to be set within the licences, and the size and existing business practices of firms impacted. However, costs could be incurred to meet requirements in different areas, for example, the cost of hiring additional staff to provide specific support to vulnerable consumers.

- **Licence application**: This is the direct cost or fee associated with applying for the licence. For illustration, the heat networks future market reform IA assumes a one-off cost of £634 per firm[22].

- **Monitoring and reporting**: Organisations may incur costs to meet monitoring or reporting requirements for either NIS requirements or the new licence.

    - **NIS**: Organisations may incur costs of reporting cyber breaches to the competent authority, and reporting on how they are meeting NIS requirements using the CAF. Sources found the reporting cost per incident to be £54[23], and the number of estimated in-scope incidents per year to be 39[24].

    - **Licensing**: Organisations may incur costs of completing data requests or developing technical solutions to automate data sharing with a regulator.

- **Pass-through enforcement costs**: Administrative costs a regulator incurs through enforcing regulations, passed through to business, such as through upkeep licence fees.

- **Learning, familiarisation and compliance**: Understanding new legislation, recruiting additional staff, demonstrating compliance.

    - **NIS**: The NIS 2020 PIR suggests familiarisation costs of £655 per firm[25] and ongoing additional compliance costs of £80 for small, £275 for medium, and £549 for large firms[26].

    - **Licence**: Evidence suggests ongoing familiarisation and compliance of a licence is £740 per year per firm[27].

- **Governance**: This includes the resource costs from supporting the development of these arrangements.

Benefits:

- **Reduced risk of cyber-attack**: For example, via a reduction in the scale and frequency of a breach. The average cost of a cyber security breach to a business is £1,570, and the number of breaches in scope of NIS is estimated to be 39 each year[28]. Larger firms may anticipate larger costs and therefore larger potential benefits. These figures exclude wider system cascading impacts and benefits and may underestimate true

[22] This assumes a senior manager taking on average 24 hours to apply for the licence, at a wage of £26 per hour. It is not certain how this would translate to our proposals.
[23] Depends on the current amount of incident reporting, how many incidents may need to be reported in the future, and the cost of reporting this to the competent authority. Assumes 45 minutes of an IT professional's time to collect and present the information; 45 minutes for legal clearance; and 20 minutes for managers or senior directors to approve the notice at average wage rates from ASHE (2016-2018).
[24] Networks and Information Systems Regulations: Impact Assessment (2018)
[25] Assumes legal takes 12 hours, and IT directors take 6 hours to familiarise with legislation and guidance docs at wage of c.£25 and c.£33 per hour respectively
[26] Assumes legal takes 10 hours, and managers take 14 hours to comply, at wage of c.£25 and c.£21 per hour
[27] Heat networks future market framework IA. Assumes legal takes 10 hours, and managers take 14 hours to comply, at wage of c.£25 and c.£21 per hour
[28] Networks and Information Systems Regulations: Impact Assessment (2018)

costs. For example, the knock-on costs to society and businesses of a cyber-attack, associated with a loss of provision of essential services, are not included[29].

- **Increased market size**: Increased consumer confidence drives demand for DSR services and the size of the market for load controllers to sell to/operate. More specifically, interoperability with ESAs will ensure that DSRSPs can offer services to any consumer with an interoperable ESA without the need for bi-lateral contracts with ESA manufacturers, increasing the potential market size. Whilst ESA interoperability can increase overall market size, it could reduce market share for some companies, and increase for others.

- **Reduced service development costs**: There may also be benefits to DSRSPs from standardised ESAs, where they avoid costs of developing best-practice or engaging bilaterally with other firms.

- **Reputational**: By reducing the risk of cyber-attack via sufficient cyber security spending, firms may experience a reputational benefit.

Energy suppliers

This group includes organisations responsible for supply of electricity to consumers. Energy suppliers will be impacted by proposals to make time-of use tariffs available in an interoperable way (Chapters 3-4). Some energy suppliers may also act as DSR service providers. These impacts are described under the load controllers heading above. Some of the impacts they may face, and illustrative examples are:

Costs:

- **Transition**: One-off costs of changing processes, such as the initial costs of developing technical frameworks for time-of-use tariff interoperability

- **Ongoing delivery**: Ongoing costs to maintain and deliver solutions for time-of-use-tariff interoperability.

- **Governance**: This includes the resource costs from supporting the development of these arrangements.

Benefits:

- **Reduced cost of technical solution (e.g. Time-of-use (ToU) tariffs):** Benefits may arise as processes are simplified and standardised, avoiding costs of developing bespoke solutions.

- **Increased market size**: Energy suppliers may be able to market time-of-use tariffs to a wider group of consumers.

[29] The Cambridge Centre for Risk Studies (2016) modelled a loss of electricity supply from an attack affecting between 9 million and 13 million electricity customers. The knock-on effects include disruption to transportation, digital communications, and water services for 8 to 13 million people.

Energy system/network operators

These groups include distribution network/system operators, transmission network operators and the Electricity System Operator (and the Future System Operator, when in place[30]), who are responsible for delivering, maintaining, and operating parts of the energy system. They will be impacted by all proposals set out in the consultation.

Costs:

- **Governance**: Organisations will be required to participate in processes to determine what requirements are needed on devices and organisations to ensure system stability.

Benefits:

- **Increased system stability**: Ensuring organisations and devices are appropriately cyber secure and mitigate risks to grid stability will reduce the risks of system stability being compromised, and the wider negative impacts to these organisations from these incidents, such as blackouts. Case studies such as August 19th (2019), Cambridge Centre for Risk paper (2019), Storm Arwen (2021), Storm Uri (2021) demonstrate the range of costs from blackouts, despite their cause[31]. This represents the possible costs avoided by cyber security to mitigate grid stability risks.

- **Reputational**: By increasing the stability of the system, system operators may experience reputational benefits.

Government and regulators

Government and regulators, such as Ofgem, will incur costs from developing and implementing the regulatory requirements proposed across the consultation. Some of the impacts government and regulators may face, and illustrative examples are:

Costs:

- **Policy development and implementation**: Costs of developing policy frameworks and regulatory requirements. Costs include recruiting staff, procuring technical services and potential legal, consulting and business services.

- **Monitoring and enforcement**: Administrative burden on government and regulators from delivering regulatory regime. This will be impacted by the enforcement body and mechanisms to be decided at secondary legislation.
    - **NIS**: Ofgem and BEIS will incur costs from fulfilling their roles as joint Competent Authority, such as resourcing costs arising through identifying operators in scope, publishing guidance, assessing and inspecting existing practices, receiving incident reports and enforcing the framework. Historic costs to BEIS and Ofgem acting as the Competent Authority under the NIS are reported as one off implementation costs of £1.08m and annual costs £1.14m[32].

[30] BEIS, Ofgem. Future System Operator Consultation Response (2022)
[31] August 2019 blackout, Cambridge Centre for Risk paper (2019), Storm Arwen (2021), Storm Uri (2021)
[32] Post-Implementation Review of the Network and Information Systems Regulations 2018 (2020).

Central Bodies (if needed to deliver proposals)

Central bodies could be needed to deliver proposals related to the technical framework (Chapter 4) and participate in governance (Chapter 5). Common systems needed could include Public Key Infrastructure or systems for anomaly detection, amongst others. Central bodies could also provide other common services, such as co-ordination of governance arrangements or assurance schemes.

The costs incurred by any central bodies will depend on the role of any central body and the common systems or services it provides, which are not proposed in detail in the consultation. However, if central bodies are needed, costs could include:

Costs:

- **Set up costs**: Initial costs to establish central bodies or equip an existing body for the role, such as appointing staff, establishing governance arrangements and investing in core capabilities.
- **Ongoing administrative and governance costs**: Ongoing costs of administering any central capabilities needed, such as providing secretariat functions, managing procurements and contracts, and providing essential IT and/or HR functionality.
- **Delivery of common systems or services**: Provision of central systems or services will incur direct costs, such as capital costs of system, support staff costs, licenses, amongst others. There will be significant variance depending on the exact role of the central body.

This analysis does not propose any specific benefits incurred by central bodies themselves. However, it is recognised that these bodies can enable benefits to other groups – such as reduced duplication of activities performed by ESA manufacturers/load controllers, or benefits associated to improved overall system security.

Consumers

This group includes all consumers and those who buy and use energy smart appliances or participate in services involving remote load control. Consumers will be impacted by proposals for ESA requirements (Chapter 3-5), smart mandate (Chapter 6) and licensing (Chapter 7). Some of the impacts they may face, and illustrative examples are:

Costs:

- **Pass through costs of meeting regulatory requirements**: Organisations in scope of regulatory requirements may pass on some of their increased costs (described in other sections) to consumers through higher product or service costs.
- **Reduction in consumer choice**: This cost may appear via removal of certain products from the market, such as non-smart heat pumps.

Benefits:

- **Bill savings**: As described elsewhere in this document, increased system flexibility reduces the overall cost to the energy system. This cost reduction benefits all consumers, including those who do not use ESAs or participate in DSR directly, via reduced bills. For example, there is evidence from a range of sources (e.g Smart Systems and Flexibility Plan, Carbon Trust)[33] that DSR and the flexibility provided by smart appliances will reduce the need for network reinforcement. The CrowdFlex[34] study concluded that DSR could reduce peak electricity demand by up to 23%, reducing costs to the energy system in turn and ultimately these savings will be passed on to consumers.

- In addition, new functionality and increased consumer confidence enabled by these consultation proposals will allow consumers to make use of time-of-use tariffs and other propositions for DSR, reducing their individual bills further.

    - **Smart mandate (Chapter 6):** Compared to a non-smart equivalent, the annual heating bill for a low-temperature air source heat pump could be reduced although the exact benefits will depend on what tariffs are available and consumer behaviour.

    - **Time-of-use (ToU) tariff interoperability (Chapter 3-4):** Benefits of ToU tariffs may vary greatly in terms of savings across different types of home, and therefore current evidence is limited. Although these savings would depend on pricing decisions made by energy suppliers at a point in time.

    - **ESA standards (chapter 3-5):** ESA standards will ensure ESAs have the capabilities to be used for DSR, allowing consumers to access rewards in exchange for providing flexibility. The size of these rewards will depend on the ESAs the consumer has, the capabilities of the ESA (e.g. frequency response or V2G) and consumer preferences.

- **Consumer choice**: Proposals for ESAs to be interoperable with DSRSPs and ToU tariffs will ensure ESA consumers can take advantage of new offers, rather than being locked in.

- **Cyber security**: Mitigating risks of cyber-attack can avoid loss of personal data or mis-use of devices for consumers using ESAs. All consumers, including those not participating in DSR or using ESAs also benefit as increased cyber security reduces the risk of cyber-attack and improves grid stability.

- **Consumer protection**: Consumer protection risks should be mitigated, for example by licensing requirements, reducing likelihood of consumers suffering from poor customer service, lock-in or unfair terms.

[33] These sources are discussed under the “Benefits of Demand Side Response” section

[34] The CrowdFlex study (2021) investigated how 25,000 households responded to price signals by reducing or increasing electricity demand, by National Grid ESO, Scottish and Southern Electricity Networks Distribution, Octopus Energy, and Ohme.

Distributional impacts

Consumers are expected to benefit from these proposals in many ways, such as reduced overall costs, increased access to different services, and reduced risk of detriment. This section considers whether these consultation proposals are likely to disproportionately impact specific consumer groups. Project Involve provides further discussion of specific impacts on low income or vulnerable consumer groups from smart energy technologies more generally[35].

Based on analysis to-date, the following distributional impacts have been identified:

- **Increased costs**: Proposals that increase the potential cost of products or services could raise barriers to low-income consumer accessing these products or services.
- **Product/service complexity**: Consumers may require digital literacy and other skills to confidently use ESAs and participate in services involving DSR. Proposals in the consultation to promote uptake of ESAs and DSR may increase inequalities between consumers who can and cannot access these products and services.
- **Locational barriers**: Consumers may incur barriers to using ESAs or DSR based on their location or the state of their premises. For example, consumers may require appropriate internet connectivity to participate in certain types of DSR requiring continuous communications between devices and service providers. Furthermore, consumers in rented accommodation, social housing or rural areas may incur barriers to installing and using ESAs.

However, it is also recognised that proposed measures in the consultation will have positive impacts on disadvantaged consumer groups. For example, licensing proposals in Chapter 7 will allow requirements to be established that protect vulnerable consumers and improve accessibility. In addition, measures to promote uptake of time-of-use tariffs and DSR from ESAs will enable low-income consumers to reduce their bills, in exchange for using their appliances in a smart and flexible way. And all will benefit from reduced overall system costs, facilitated by an increase in DSR.

[35] Some other potential risks are discussed here: Project InvoLVe, BEIS commissioned. How can innovation deliver a smart energy system that works for low income vulnerable consumers? (2021).

Section 4: Questions

There are several key evidence gaps, which we wish to gather evidence from stakeholders on to inform future policy development. The key questions for stakeholders, to help address the existing evidence gaps are summarised below.

Overarching

1. **Do you agree with the case for intervention and the market failures we have identified. Are there any points we have missed?**

2. **What is your assessment of the current state of the DSR and ESA markets? What firms are operating in these markets, what products and services are being offered, and for example, to what extent are firms in the electric heating market already offering smart options?**

3. **How do stakeholders anticipate the DSR and ESA markets will grow to 2050? We would be interested in views on changes in types of firms in the market, their sizes and business models, and speed of market growth.**

4. **Do you agree with the benefits of DSR we've identified and how do you see these changing over time?**

5. **Given the challenges of measuring the benefits of cyber security, due to under reporting breaches, uncertainty of scale, and far-reaching impacts, as discussed in the 2018 NIS impact assessment, how do we best quantify the benefits of additional cyber security?**

ESA manufacturers

6. **Are the costs and benefits identified for ESA manufacturers (e.g., smart heat pumps or smart white goods) accurately specified? Are there any we've missed, or not accurately specified?**

Load controllers

7. **For firms in scope of the licence proposals, what type of costs and benefits might be incurred from these proposals?**

8. **For larger load controllers, in scope of the NIS extension proposal, are the costs and benefits identified appropriate? Are there any we have missed, or not accurately specified? For example, what is your current level of cyber security spending, and what additional spending would you anticipate in using the CAF to comply with NIS? Are you able to separate costs into categories, such as familiarisation, compliance reporting and incident reporting, or any others?**

9. For all load controllers, how much do organisations consider the risk from a cyber-attack on their activities of impact to the wider energy system?

Energy suppliers

10. Are the costs and benefits identified for energy suppliers appropriate? Are there any we have missed, or not accurately specified?

Consumers

11. Are the costs and benefits identified for consumers appropriate? Are there any we have missed, or not accurately specified?

Distributional Impacts

12. Do you have a view, and supporting evidence, on the impact of the proposals on different consumer groups, for example low income and vulnerable consumers? What further action is needed to ensure all groups can benefit?

Next steps

The evidence gathered from stakeholder responses will be used to inform future policy proposals. Any future legislative proposals will be accompanied by detailed impact assessments, as required.

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 to: SSESconsultation@beis.gov.uk

or

Write to:

SSES
NZEN
Department for Business, Energy and Industrial Strategy

3rd Floor
1 Victoria Street
London
SW1H 0ET

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.