Department for
Energy Security
& Net Zero

Delivering a smart and secure electricity system

Government response to the 2022 consultation on interoperability and cyber security of energy smart appliances and remote load control

March 2023

Contents

Executive Summary

Vision: enabling consumers to take more control of their electricity use

Through the decisions confirmed in this publication, the Government is taking an important step towards creating a smart and flexible electricity system, by helping unlock the potential for consumers to benefit from using smart technology to shift the time that they use electricity. This will minimise consumer bills, enable the growth of the UK's smart technology sector, and help meet our energy security and net zero targets.

The decisions in this consultation response will help ensure consumers can use a wider range of services and devices in homes and small businesses to manage their electricity consumption and reduce bills. For example, heat appliances like heat pumps and heat batteries will have smart functionality. This will mean that a heat pump can be used, or heat battery charged, automatically during times when electricity is cheapest. Homes with an electric vehicle charge point installed will have a greater choice of regulated third parties that can offer them lower bills, or other incentives, for charging their car at certain times of the day.

In addition to these consumer benefits, the action set out here will help support UK businesses and economic development. Use of smart systems and flexibility could create 10,000 jobs and increase GDP by up to £1.3bn by 2050. A further 14,000 jobs could also be created by the export potential of these technologies.[1] Our proposals will help some of these economic benefits become a reality by unlocking the potential of domestic-scale consumers to contribute to a flexible electricity system. Making a wider range of energy smart appliances and associated services available to consumers will help create the conditions for a competitive, innovative market and set the groundwork for it to grow.

Finally, these measures will contribute to a cleaner, more secure and cheaper electricity system, which overall we expect will reduce electricity system costs by £6-10bn per year by 2050[2]. The measures will ensure that uptake of energy smart appliances and associated services do not cause problems with the stability of the grid, and reduce cyber security risks that online connected energy smart appliances could pose.

A smart flexible electricity system

As we transition to a clean, net zero electricity system, the way we generate and consume electricity will change. Whereas historically, at times of high electricity demand, more fossil fuels were consumed to generate more power, renewable energy is more dependent on the weather. This will mean that excess power is available at times when there is low demand, but also that there are times when solar panels and wind turbines will generate less power. To address this, we can build more physical infrastructure but we can also create a smart and

[1] These benefits could be achieved through a combination of demand-side response, interconnectors and energy storage technology. Smart Systems and Flexibility Plan 2021

[2] Ibid

flexible electricity system where we are able to match electricity supply and demand efficiently. This can be done through “demand-side response" (DSR).

DSR means consumers can continue to use electricity when they need it but have the option to make changes in their electricity consumption patterns and save money in return. Some of these services are being provided today; for example, electric vehicle (EV) owners can get discounts or cash-back by charging their car during periods of the day when electricity demand is low. Not all demand can be shifted – for instance, people will need to light their homes when it is dark, and cook when they want to eat. However, as we electrify our economy and electric vehicles and electric heating become widespread, there will be many more opportunities for consumers to shift some of their electricity consumption through DSR.

If DSR is taken up by many consumers in the future, it can provide substantial benefits. By flattening peaks in overall electricity demand, DSR can reduce electricity system costs and energy bills, contribute to security of supply, and make it easier for the electricity network to accommodate intermittent renewables.

Policy context

In July 2022, the Government published a consultation focused on unlocking greater use of domestic and small non-domestic scale DSR. There are currently barriers and risks related to the growth of the domestic and small non-domestic DSR market. For the market to grow, communications between devices and services and how tariff information is shared need to be standardised. This will mean a wide range of DSR services can be offered and easily accessible to all domestic and small non-domestic consumers. Without this, consumer access to DSR services may be limited to certain service providers or manufacturers of devices. Government also needs to ensure there are consumer protections in place to build confidence in the developing market and ensure fair contractual arrangements are in place so the benefits of DSR are passed onto consumers. In addition, greater use of energy smart appliances and other associated services could pose risks to the energy system, such as creating new vectors for cyber attacks and threats to grid stability. With many devices already internet-enabled, those risks will increase without government intervention.

The Government’s July 2022 consultation set out proposals in three key areas to address these barriers and risks:

- Creating the right technical frameworks to unlock the potential of flexibility for domestic and small non-domestic energy consumers.
- Improving the security of the electricity system.
- Giving consumers confidence to engage with a smart energy system.

Responses to the July 2022 consultation broadly supported the Government’s proposals. This document confirms the Government’s intention to progress with the proposals and sets out next steps, including our plans for further consultation on points of detail.

Consultation responses and decisions

The Government received a total of 84 responses to our July 2022 consultation from a mix of parties, including manufacturers, energy suppliers, network operators, technology companies, consumer groups and other stakeholders. The Government conducted 33 engagement events online and in-person between July and September 2022 to gather a wide range of views on our proposals. These events aimed to raise awareness of the consultation's proposals, help Government to obtain feedback on them, and support participants to develop their own responses to the consultation.

We are grateful for the helpful information provided at these events, alongside views set out in formal consultation responses. In the development of this consultation response, we have considered and reflected on the feedback received. A summary of themes from consultation engagement alongside key decisions taken within this document is provided in the tables below, after which we set out how the actions we are taking will collectively benefit consumers, industry and the energy system:

Consultation proposals on the use of the Network and Information Systems Regulations (2018) to improve cyber security of the energy system	
Consultation responses indicated support for applying the Network Information and Systems Regulations to load controllers[3], and the need to introduce a threshold for applying these regulations. A range of additional metrics were put forward in regard to the proposed 300MW threshold.	
Following the consultation, we confirm our intention to:	We commit to consulting in further detail on:
• Bring load controllers into the scope of the Network and Information Systems Regulations. • Use a 300MW threshold for load controllers to be considered Operators of Essential Services under the Network and Information Systems Regulations. • Use the Cyber Assessment Framework as a means of assurance in relation to the security duties under the NIS Regulations. • These proposals are subject to Parliament granting powers to amend the NIS Regulations, as set out in Government's proposal for legislation to improve the UK's cyber resilience[4]	• Changes to the NIS regulations using delegated powers, as set out in the Government's response to the call for views on proposals to improve the UK's cyber resilience[5] (subject to Parliament granting the power to amend the NIS Regulations).

[3] organisations remotely controlling electrical load using communication networks.

[4] Proposal for legislation to improve the UK's cyber resilience: Proposals to future-proof the UK NIS Regulations

[5] Government response to the call for views on proposals to improve the UK's cyber resilience

Consultation proposals on the outcomes, technical frameworks, and delivery frameworks for energy smart appliances
Consultation responses indicated wide support for the proposed outcomes that energy smart appliances (ESAs) should meet. A range of questions and challenges were raised in relation to how to meet the proposed outcomes in practice. Responses also indicated support for proposals to require compliance with ESA standards, and to standardise time-of-use tariff data. There was a mix of views on how to implement regulation to support energy smart appliances, as well as details on what should be part of minimum cyber security requirements, and the role of common systems to mitigate cyber security risks. There was also a mix of views on the best approach to governance arrangements and cost recovery process for meeting ESAs standards.

Following the consultation, we confirm our intention to:	We commit to consulting in further detail on:
• Use our proposed interoperability, cyber security, grid stability and data privacy “outcomes” to inform future regulation of energy smart appliances. • Require energy suppliers to make time-of-use tariff data openly available in a common format, over the internet. • Require compliance with standards for energy smart appliances, including EV charge points, batteries and heating appliances, through proportionate regulation. • Work with industry and BSI to develop a standard, based on PAS 1878, for the future regulation of energy smart appliances. • Require compliance with minimum cyber security requirements for energy smart appliances, using the ETSI 303 645 standard, in advance of longer-term standard developments.	• Our implementation governance approach. • The approach to mitigating grid stability risks from energy smart appliances. • The details of the assurance approach for energy smart appliance standards. • The role of common systems to mitigate potential system-wide risks from energy smart appliances. • Our cost recovery approach. • The technical and governance solution for interoperability of time-of-use tariff data.

Consultation proposals on mandating smart functionality in electric heating technologies
Consultation responses were supportive of the proposal to mandate smart functionality for hydronic heat pumps, storage heaters, and heat batteries. The majority of stakeholders indicated that they would like to see the mandate extended to additional electric heating

appliances, as well as domestic-scale batteries. Respondents were generally content with our proposed timing for the mandate but provided mixed views on whether 2025 would leave enough time for products to be made compliant.	
Following the consultation, we confirm our intention to:	We commit to consulting in further detail on:
• Mandate that hydronic heat pumps, storage heaters and heat batteries should have smart functionality, meaning they should be able to provide demand-side response. • Implement the smart mandate proposal alongside the first phase ESA regulations in the mid 2020's (2026-27).	• The potential for additional requirements to be placed on smart electric heating appliances. • The potential to extend the smart mandate to further electric heating appliances.

Consultation proposals on regulating organisations with a role in managing electrical load control through a licensing regime	
A significant majority of responses to these proposals agreed on licensing DSR service providers. Responses also indicated support for the proposed scope of the licensing regime applying to those controlling ESAs of domestic and small non-domestic consumers. A range of views were expressed on how the licensing regime should be set up, with most agreeing that it should be flexible and proportionate. Most also agreed that the licensing regime should consider measures protecting consumers, cyber security, interoperability and grid stability.	
Following the consultation, we confirm our intention to:	We commit to consulting in further detail on:
• Develop a new licensing framework for organisations carrying out DSR, focussed on domestic and small non-domestic consumers. • Focus the licence, at least initially, on the relationship between domestic and small non-domestic consumers and demand-side response service providers (DSRSPs). • Base our development of the licencing framework on the design principles set out in the consultation, with additional suggestions from stakeholders being kept under review.	• How we define small non-domestic consumers and load control actions to include in the licensing scope. • Defining a proportionate approach for licensing conditions depending on the extent of risks posed to consumers and the grid. • Possible additional protections for consumers and data privacy. • Possible provisions to ensure cyber security of load controllers that are below the 300MW threshold for the

	Network and Information Systems (NIS) Regulations requirements. • Interoperability gaps such as contractual lock-ins. • Controls to ensure grid stability from DSRSP load control activities. • Delivery and implementation of the licensing regime.

How our decisions achieve the key aims we consulted on

Below we set out how the actions confirmed in this document help meet the aims of our July 2022 consultation, and our measures means in practice for consumers, industry, and the energy system. Further details on next steps across our proposals can be found in the “Stakeholder engagement & next steps” section of this document.

Creating the right technical frameworks to unlock the potential of flexibility for domestic and small non-domestic energy consumers.

Energy smart appliances, such as EV charge points, heat pumps and batteries, have significant potential to provide value to the energy system through flexibility. The value of flexibility to consumers and the energy system will grow over time, as uptake of appliances grows and our energy system changes. However, in the absence of intervention, ESAs may not necessarily be used flexibly - either because they do not have the right technical capabilities, or because there are barriers to consumers providing flexibility through ESAs. We intend to remove some of the most significant barriers to consumers providing flexibility to the energy system.

Our interventions will ensure that appliances installed in consumer premises will have the essential capabilities needed to provide flexibility throughout their operational life. They will also ensure that consumers are not ‘locked-out’ of the best tariffs and services that incentivise flexibility, allowing them to sign-up to the services that best meet their specific needs.

Specifically, we have confirmed that certain electric heating appliances will have a minimum level of ‘smart’ functionality from the mid-2020s. We will consult on the details of these requirements later this year and expect them to be operational between 2026 and 2027. We have also confirmed that later this decade large energy smart appliances will need to use ESA standards, to deliver interoperability. This will mean that consumers can use their ESAs with a range of DSR service providers, similarly to how consumers expect to switch energy supplier or mobile network provider today. We will begin the process of developing an ESA standard later this year and aim for it to be in place by the mid to late 2020s.

In practice, implementing an ESA standard will require a significant programme of work involving industry, regulators, and government. This includes demonstrating the use of standards via the IDSR innovation programme, developing a further iteration of an ESA standard (based on PAS 1878), and establishing the regulation, assurance and governance needed to support effective deployment. In advance of these steps, we intend to accelerate the growth of time-of-use tariffs as mechanism for demand-side response. Our requirement on energy suppliers to make time-of-use tariff data openly available in a common format over the internet will help ensure that ESAs can easily integrate with different tariffs from different energy suppliers. We will consult on this later this year and expect it to be in place by 2025.

The Government is seeking legislative powers through the Energy Bill that are necessary to implement these proposals. The powers will enable the Government to regulate ESAs, including requiring certain types of appliances to be smart, setting minimum standards for smart functionality for certain ESAs, and enable the Government to license activity relating to load control.

What this means in practice:

For consumers – Consumers will be able to securely use more ESAs for flexibility, with a range of different tariffs and services. This will open opportunities for households to reduce their energy bills and support net zero.

For industry – Establishing an ESA standard; standardising the format of time of use tariff data; and setting requirements on DSR service providers via a licence, will all help create the conditions for a thriving and competitive market for DSR services.

For the energy system – Our action to increase the uptake of demand-side response will mean that over the next decade more electricity consumption will be shifted to off-peak times or periods of high renewable generation, reducing peak demand. This will reduce the need for generation and network infrastructure, and therefore the total cost of the system, and reduce emissions.

Improving the security of the electricity system.

Cyber security of the energy system is critical for protecting both lives and livelihoods. As set out above, energy smart appliances and the remote control of electrical load have the potential to revolutionise how we consume energy and decarbonise our economy, but they also come with risks. For instance, if devices are not cyber secure then at the very least, they could cause inconvenience for consumers and at worst, they could cause impacts to energy supply.

Interconnected devices that control large amounts of electrical load are becoming increasingly prevalent. Other interventions set out in this document are designed to help facilitate uptake and use of energy smart appliances. However, cyber security measures are needed to protect the system as this happens and it becomes more digitised and more connected. That is why the Government is committing to implement measures to ensure that ‘smartness’ and ‘security’ are developed in lockstep.

As a first step, we will implement new regulations to set minimum cyber security standards for ESAs. We aim to consult on these later this year, including consideration of a randomised delay functionality on ESAs to mitigate grid stability risks, prior to introducing secondary legislation for the requirements in 2024 at the earliest. This legalisation will build on learning from the ground-breaking Electric Vehicle (Smart Charge Points) Regulations 2021 and will set appropriate standards for cyber security and grid stability for a wider cohort of energy smart appliances, including smart heating appliances. We will work with industry to confirm when these regulations will come into force but anticipate this being from 2026, to allow sufficient time for industry to adapt their products to the new standards.

However, a chain is only as strong as its weakest link. In addition to making sure that devices are cyber secure, we need to ensure that the back-end systems which control these are also secure. This is why we will continue to work with technical experts within government (including the National Cyber Security Centre) and industry to develop a holistic package of longer-term measures necessary to provide end-to-end security for the smart energy system. This work will build on and complement the initial device level standards, and deliver an enduring and robust cyber security architecture to support protection of the energy system and help support consumer confidence.

While the focus of our work is on enabling cyber secure domestic-scale demand-side response services for end-consumers, we also recognise that there are other parts of the economy where large amounts of electrical load are being controlled remotely. This includes areas such as large-scale industrial and commercial demand-side response and, increasingly, public electric vehicle charging. This is why, to complement the measures outlined above, we will also seek powers to bring organisations controlling large amounts of electrical load in scope of the Network and Information Systems Regulations, using a threshold of 300MW. These regulations impose security duties on Operators of Essential Services. We will consider what other cyber hygiene may be required below that threshold including via our licensing proposals.

What this means in practice:

For consumers – cyber security requirements will be strengthened over the decade as the roll out of ESAs becomes more commonplace in households. Consumers will be able to use ESAs and related services with peace of mind.

For the energy system – cyber security protections will grow as larger amounts of remotely controlled load enter the system. These will protect against grid level disruption and ensure that ESAs can be treated as assets that provide flexibility, rather than risks to the wider system.

For industry – requirements on manufacturers and load controllers will evolve over time. Government will work closely with industry to ensure these are proportionate. It will be important that we work together to ensure that requirements map together coherently and build on each other. Each step along the way should strengthen what went before rather than meaning that it needs revisiting.

Giving consumers confidence to engage with a smart energy system.

The decisions we have made also aim to ensure consumers who decide to participate in demand-side response have confidence in the third-party devices and services that they rely on. Without our ESA standard and licencing proposals, consumers could purchase an expensive device and then find it has limited functionality as it cannot be used with different tariffs and services. Our proposals will prevent consumers being locked-in to using certain devices or services for demand-side response or locked-out from accessing the best propositions.

There is an existing marketplace for demand-side response for large energy users where mutually agreed contractual arrangements can provide assurance for both parties. However, these sorts of bespoke arrangements are unsuitable for the domestic and small non-domestic market. Just as households do not currently negotiate terms and conditions for the supply of their energy, we do not expect them to do so for demand-side response services.

In addition, our interventions aim to protect consumers from cyber security and data privacy risks from ESAs and DSR services. Through implementing protections for devices and organisations, we will ensure that consumers are better protected against their devices being compromised by malicious actors, and loss or misuse of personal data.

Our decision to set up a licencing regime for organisations providing DSR services to domestic and small non-domestic consumers will guard against unfair contractual arrangements between consumers and DSR service providers. In addition, licensing will provide a framework to ensure vulnerable customers are protected. We will consult on the initial details of this licencing framework later this year and will introduce an initial licence by 2025. Requirements of the license will develop further beyond this point to reflect the changing needs of consumers and the wider energy system. Alongside our ESA requirements, licensing will help ensure that consumers can be confident in their use of demand-side response and the benefits it will bring them.

What this means in practice:

For consumers – Users of DSR service providers will benefit from a licensing framework that ensures fair contractual arrangements. Owners of ESAs will have a wide range of choices on how they can optimise electricity consumption of these devices in a way that benefits them and aids the net zero transition.

For the energy system – If consumers have confidence in demand-side response services, their uptake will increase, reducing the costs of managing our electricity system and reducing emissions by maximising the use of intermittent renewables.

For industry – A policy framework that supports consumers who choose to use demand-side response services will increase appetite for these services, helping unlock growth in a burgeoning demand-side response services sector.

Timescales for implementation

In the consultation, the Government proposed a phased approach to implementing our proposals, with the intention of consulting in further detail on specific areas. We set out high level timescales for each proposal with consideration of when they needed to be in place to best ensure we meet our 2050 net zero target whilst considering the time needed for technology to develop, and lead in times for industry to adapt to the proposed final requirements.

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

Summary of responses

There were 61 responses to this question, out of these responses, the most common themes were broad agreement with the proposed high-level timescales (20 mentions) and broad agreement with the phasing approach (18 mentions).

Other themes included needing to be more ambitious and/or have earlier timescales on some or all of the proposals (17 mentions), and the need for more clarity on the detail of the proposals as soon as possible (14 mentions). Other common themes in responses included encouragement to engage with industry to inform the next steps and detail of proposals (10 mentions), and an emphasis on ensuring sufficient “lead in” times were in place to allow industry to comply with the proposals.

Other less common themes included concerns being raised about the possibility of energy smart appliances being rolled out that are non-compliant with the final requirements, the proposals being too ambitious in terms of timescales, and the need for proposals to be further developed as the market for flexibility services evolves.

In our engagement events Government also heard about how the successful implementation of our proposals will depend on other initiatives and necessary developments such as the introduction of half hourly settlement and the role that the Future Home Standard will play in 2025.

Government response

2025 will be a key year for DSR and flexibility services. Market-wide half-hourly settlement is expected to be introduced, alongside the Government’s Future Homes Standard. We expect this to drive a ramp up in market development for energy smart appliances. Our timescales seek to align with these expectations for uptake and delivery of DSR, while also reflecting the lead in times that industry will need to ensure they can adapt their services to the incoming requirements. Government will work with industry with a view to accelerating implementation where possible.

Below we have set out an indicative delivery plan for our proposals, including proposed timescales for further consultation, and proposed timescales for implementation.

We have largely maintained the high-level timescales as set out in our consultation, however, to ensure we have sufficient time to work closely across Government and with industry to understand the scope of cyber security requirements, we have moved our timescales for laying ESA minimum cyber security requirements back from the initially proposed “short term” timescale. In addition, we have accounted for further time needed for industry to comply with our proposed smart heat mandate. Further detail on the case for these changes can be found in the relevant chapter and question sections of this document. The final timescales of all proposals are dependent on primary and secondary legislation, which will be subject to the will of Parliament.

We will work closely with industry via technical working groups to finalise timescales and inform our policy thinking. Work with these technical working groups will also help inform Government’s approach to implementing our minimum cyber security requirements and smart mandate prior to introducing an ESA standard. We will work with industry to introduce these requirements in a manner which minimises industry disruption. Further information on our plans for future consultation across our proposals and on how we will work with industry and other stakeholders to inform next steps is in the "Stakeholder engagement & next steps” section of this document.

*Proposal /Indicative timeline**	**2023**	**2024**	**2025**	**2026**	**2027**	**2028**
Development and adoption of an ESA standard	Primary legislation put in place Further detail of proposals to be consulted on	Secondary legislation developed		Window for proposals to become operational		
Introducing the "smart mandate" to heat technologies	Primary legislation put in place Further detail of proposals to be consulted on	Secondary legislation developed		Window for proposals to become operational		
ESA minimum cyber security requirements						
Tariff interoperability		Secondary legislation developed	Window for proposals to become operational			
Introducing a licensing regime				*Window for potential further changes to licence to be made reflecting on implementation of other proposals.*		
Expanding the scope of the Network and Information Systems Regulations 2018 to include certain load controllers	Primary powers to amend NIS Regulations put in place Consultation, as appropriate, on changes to NIS Regulations Secondary legislation developed		Window for proposals to become operational, supported by the Cyber Assessment Framework			

*Timeline indicative only, implementation dependent on legislation. Window for proposals to be operational reflects potential lead-in times for industry to prepare for compliance, for example making any changes to manufacturing processes and supply chains.

Cyber security proposals for protecting the energy system

Within this chapter of the consultation, the Government sets out its proposed approach to cyber security for organisations remotely controlling electrical load using communication networks (‘load controllers’). It explained the strategic context to this approach, the services provided by load controllers in a dynamic energy system, and the role of the Network and Information Systems (NIS) Regulations (2018) in raising the cyber security of specific critical sectors. Government proposed that i) load controllers managing loads that have the potential to cause significant disruption to the electricity system are brought within the scope of the NIS Regulations, ii) load controllers remotely managing 300MW or more should be considered Operators of Essential Services (OES) and therefore subject to obligations under the NIS Regulations, and iii) that the Cyber Assessment Framework (CAF) is used to assess compliance.

Proposal

Question 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.

Question 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.

Summary of responses

We received 56 responses to question 2 and 43 responses to question 5.

48 respondents agreed that load controllers should be subject to the obligations in the NIS Regulations. 7 responses were neutral, and 2 responses disagreed. Across all types of organisations, responses showed recognition of the significant, and growing role of load controllers in the electricity sector, and the high impact a compromise of a load controller could have on the electricity system. Among responses there were references to factors that could be included in the design of the proposal, including monitoring compliance, and the need for clear definitions of the scope in legislation and guidance.

Several responses called for further impact assessments and analysis from Government, and some responses asked that the approach to implementation and associated costs be proportionate to the risk an organisation could present to the electricity system. Some respondents noted a need for more technical expertise in the sector in order to implement the proposal, and a need for more cyber security skills in the market.

Of 43 responses to question 5, 35 agreed with Government's proposal to use the CAF to support the implementation of the NIS Regulations requirements for load controllers, 7 responses were neutral and 1 disagreed. Responses that were in agreement or neutral cited the CAF as an already established and recognised framework and supported its outcome-focussed approach. Almost one quarter of respondents who agreed highlighted that the approach taken to assurance and enforcement using the CAF will be critical in how effective it is at supporting risk management. Some responses raised the view that guidance on assurance and compliance would help avoid ambiguity, inconsistency, and costs.

Government response

The amount of electrical load controlled by organisations providing DSR will increase as flexibility increases, and remote load control as a function will become a growing part of other businesses. As load controllers (organisations carrying out load control[6]) provide services to a more flexible electricity system, the associated increase in digitalisation and remote energy management will bring new cyber-security risks, with higher associated impacts to the electricity system and end consumer. Without an appropriate level of cyber security, load controllers could become a point of vulnerability in the broader electricity system.

We intend to bring certain load controllers into scope of the NIS Regulations, subject to the will of Parliament, using the CAF to support assurance against relevant NIS Regulations requirements. To enable this, we will seek powers to amend the NIS Regulations so that we can subsequently use those powers to extend the obligations under those regulations to relevant load controllers. In Government's response to the call for views on proposals to improve the UK's cyber resilience[7], we have already committed to bringing forward new primary legislation to make it easier to ensure the NIS Regulations can keep pace with the evolving cyber security landscape. This will be introduced when parliamentary time allows. On the assumption that enabling powers to make delegated legislation in the future are secured, any proposed future amendments to the NIS Regulations in relation to load controllers will be consulted upon.

The approach to implementation of any new obligations under the NIS Regulations in relation to load controllers will be informed by consultation responses, additional risk assessment work that will be carried out with the National Cyber Security Centre (NCSC), and engagement with Ofgem, network operators and load controllers operating in the market.

As an outcome-focussed framework, Government considers the Cyber Assessment Framework (CAF) appropriate to support the assurance of requirements under the NIS Regulations for a nascent, varied and evolving market. This is because it does not prescribe how each outcome should be achieved, thereby allowing for change in a sector and variation in organisation.

[6] Load control is the activity of configuring or controlling the consumption, discharge or production of electricity of devices.

[7] https://www.gov.uk/government/consultations/proposal-for-legislation-to-improve-the-uks-cyber-resilience/outcome/government-response-to-the-call-for-views-on-proposals-to-improve-the-uks-cyber-resilience

Load controllers will play an increasingly essential role within the electricity system, in providing flexibility services to our Critical National Infrastructure (CNI), and services to consumers. Amending the NIS Regulations so that certain load controllers could be designated or deemed to be designated an OES would reflect this significant role they will play in a highly connected electricity system. As we set out in July 2022 consultation, based on cross-sector analysis, we do not believe that the market alone is an adequate driver of appropriate and proportionate cyber security. It remains Government's view that intervention is necessary to manage cyber security risks appropriately and proportionately, especially in critical sectors such as energy. The NCSC has assessed that voluntary, industry-led codes are unlikely to drive the level of adequate, consistent cyber security resilience necessary for managing the risk of cyber-attack in the longer-term.

Threshold and Metrics

Question 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.

Question 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?

Summary of responses

We received 45 responses to Question 3 and 43 responses to Question 4.

A significant majority of respondents to Q3 agreed that there needed to be a threshold. 14 responses supported the 300MW proposed, and 6 were in favour of this alone as a threshold. Several responses gave support to a threshold that represents the point at which an organisation's compromise could impact grid stability and sector Critical National Infrastructure (CNI). 28 responses were neutral on the proposed 300MW. 5 responses disagreed with the 300MW load threshold proposed, some citing the inability of load controllers to control all the load within their portfolio as a concern, and others citing concerns over the risk present in the system at load levels lower than 300MW should organisations managing smaller loads be compromised.

37 responses put forward other metrics or additions to the methodology for consideration. Most frequently raised among these responses were i) the variability in risk and impact caused by the geographical concentration of load, including consideration of impacts from lower levels of load on the lower voltage parts of the grid, and ii) the impact of different business models for load control (including proportion of flexibility held, configuration of different charging stations, how the threshold would differentiate between multiple and single sites held by the same organisation, and varying types of generation). Building on (ii), some respondents proposed consideration of the total power consumed by the devices controlled at any one time, relative to the business model of the load controller. For example, of the total load a charge point

operator is capable of controlling, the actual load controlled will vary over time. Suggestions to capture metrics on the number of customers or households connected were also put forward. A small number of respondents wanted any threshold to be kept under review, to ensure it can continue to reflect the critical mass at which load controllers could impact grid stability. Some respondents put forward suggestions for a graduated threshold, or for using multiple thresholds simultaneously.

Government Response

Subject to delegated powers being granted by Parliament, we intend to recognise load control as an essential service, and designate OES using a threshold or where they are designated by Government as OES on other grounds under the alternative power in Regulation 8(3). We intend to set the threshold at 300MW. This proposal takes into account the point at which a load controller could have an unacceptable impact on the electricity system, and our critical national infrastructure. The proposed threshold of 300MW reflects Government's current intention, our knowledge of the electricity system and the cyber threat landscape, and seeks to future-proof the NIS Regulations. We intend to keep thresholds in the NIS Regulations under review in future. We will consider responses on the variability of risk amongst those designated OES when developing an assurance approach using the CAF. The CAF will enable an approach that is scalable across diverse organisations, allowing them to meet cyber security outcomes in a way that is proportionate to their own operations.

We recognise the need for a systemic approach to risk management, and this document sets out our intention to develop cyber security requirements that could apply to organisations not in scope of the NIS Regulations, including via our proposals for licensing organisations controlling loads less than 300MW and energy smart appliances. We are working to achieve consistency and compatibility across different cyber security requirements as we develop these. We will carry out further risk assessment work and business engagement to build a more detailed understanding of organisations operating in this market.

Energy smart appliances: Outcomes

Within this chapter of the consultation, the Government set out the outcomes we intend to promote in future policy for energy smart appliances (ESAs). It included a summary of the objectives of these proposals and a description of how ESAs can be used to provide demand-side response (DSR). It described 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 were also proposed.

Interoperability

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

The consultation proposed to prioritise ESA interoperability where there is a clear consumer or energy system benefit, whilst still allowing space for innovation. We proposed to ensure energy smart appliances can receive and respond to time-of-use tariffs from different energy suppliers; and provide DSR services with different DSR service providers. This aimed to protect consumers from being unfairly ‘locked-in’ if their preferences or circumstances change, or ‘locked-out’ from the best deals.

Summary of responses

Of the 56 respondents to this question, 48 agreed with the proposed outcomes, whilst 4 were neutral and 4 disagreed. Those who agreed generally recognised the stated consumer and energy system benefits from facilitating these types of interoperability. Several respondents also recognised the benefits to innovation of taking a targeted approach to interoperability, such as reducing potential impact to ESA manufacturers. However, some respondents caveated their support with the need to enable innovation, support product differentiation and limit additional cost.

Some respondents noted they did not believe that the interoperability of DSRSPs should be progressed, due to the technical challenges from delivering interoperability in practice, lack of consumer demand for DSR services and potential negative impacts on product differentiation of ESAs.

A small minority of respondents believed that the scope of interoperability should go further than the consultation proposals, potentially to include ESA operators, or Home Energy Management service providers. However, many respondents agreed that these other types of interoperability were not necessary to deliver the required benefits. Some respondents specifically noted the growing role of 'type-of-use'[8] tariffs in facilitating DSR from ESAs, suggesting that these should also be included.

Government response

Government maintains its view that removing barriers to interoperability of time-of-use tariffs and DSR services will be essential to promoting growth in markets and consumer demand for these propositions. Given the high level of support, Government plans to take forward the proposed interoperability outcomes for ESAs. This will ensure that consumers aren't locked-in to certain tariffs or services, or locked-out of the best deals, promoting greater flexibility from ESAs. In addition, we will consider how interoperability with DSR services can accommodate interoperability with 'type-of-use tariffs' across our future technical and policy frameworks, recognising the important role these tariffs may play in the future. With the exploration of innovative domestic demand-side flexibility propositions (tariffs, products and services) for a future energy system supported through the Government's £18m Alternative Energy Markets Innovation Programme[9].

Cyber Security

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

In addition to proposals for organisations controlling large amounts of electrical load to meet cyber security requirements, the July 2022 consultation also sets out proposals to protect against other cyber security risks at the device and system level. The consultation recognised that cyber incidents could damage network infrastructure, consumer confidence, and adversely affect the uptake of DSR.

In the consultation, we sought views on 8 security outcomes that ESAs may need to deliver.

Summary of responses

Of the 47 respondents, 40 were in broad agreement, 3 offered a neutral opinion and 4 disagreed with the proposed outcomes. Those who agreed commented that the proposals were a sensible starting point for cyber security, and almost half of respondents provided additional areas for the scope of the regulations, such as 'end-to-end' security. Respondents who offered a neutral position commented that there wasn't enough information for them to give an opinion, whilst those that returned negative responses focused on the positive impact of market solutions and the burdens of regulation to manufacturers.

Government response

[8] A 'type of use' tariff is an energy tariff where prices are differentiated depending on the purpose of the energy use (for example, the unit rate for energy used to charge an EV may be less than for the rest of the premises). Typically, these reduced tariffs are provided on the condition of the device being available for use for DSR.

[9] https://www.gov.uk/government/publications/alternative-energy-markets-innovation-programme

Government plans to use the proposed outcomes for cyber security to inform future technical and regulatory frameworks for ESAs. Work is also underway across Government to assess system, device, and organisational level cyber security risks, as referenced in the July 2022 consultation. The outcome of these cyber security risk assessments will also be used to inform the detailed security requirements for ESAs. The exact nature of proposed cyber security requirements and controls will be subject to ongoing engagement with stakeholders, including the National Cyber Security Centre.

Data Privacy

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

For data privacy, Government proposed that future policy should aim to meet three outcomes:

- avoid the unnecessary collection or transmission of personal data;
- minimise the amount of personal data shared with third parties (including DSRSPs);
- ensure personal data is transmitted and stored securely, with controls in place to protect against access by unauthorised entities.

Summary of responses

Of the 56 stakeholders who responded to this section of the consultation, 39 were in broad agreement, 9 were neutral and 8 were in disagreement with the proposed policy outcomes for data privacy. Comments from stakeholders focused on ensuring that the new regulations avoided duplication and/or were compatible with existing legislation. Others emphasised the importance of consumer consent for sharing data.

Government response

Government maintains the view that robust data privacy protections will be essential to protect consumers and maintain consumer confidence in ESAs and DSR. The Government anticipates that specific data privacy requirements will be needed in ESA standards to ensure these data privacy outcomes are being met (particularly when data is shared between devices, systems and organisations). The Government will continue to ensure that future ESA regulation is fully compatible with UK data protection laws and other existing legislation and will consider any interactions with our licensing framework for DSRSPs.

Given the broad agreement of stakeholders towards the stated policy outcomes, Government will proceed with designing future policy based on the proposed data privacy outcomes.

Grid Stability

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

The consultation identified specific ways in which ESAs could pose a risk to the grid, such as synchronised changes in load ('herding') of ESAs at scale, unexpected step-changes or ramps in energy usage at scale, oscillation in energy usage or production of ESAs at scale, and inability to provide the flexibility necessary to the energy system when depended on. To mitigate these risks, Government proposed that future policy should: ensure that ESAs protect against unintended synchronised changes in load; enable load-impacting settings to be remotely updated; collect and share data relevant for DSR and grid stability; and enable detection, alert and protection against communications that could negatively impact grid stability.

Summary of responses

Of the 49 respondents, 37 were in broad agreement, 9 were neutral and 3 were in disagreement. Stakeholders were in broad agreement with the need for grid stability mitigations for ESAs. However, several stakeholders noted that grid stability mitigations must be compatible with consumer needs, such as comfort, convenience, and safety, and challenged whether some of the proposed mitigations could deliver these needs. More specifically, some stakeholders were concerned that randomisation of changes in load from ESAs could erode the value consumers can achieve from time-of-use tariffs, or prevent the ESA from changing load when a consumer expects.

Some stakeholders highlighted the need to think about grid stability across the system, rather than just for ESAs. Specifically, some suggested that risk assessments must consider the diversity of service providers, ESA types and consumers, which might reduce the likelihood of devices acting in synchrony. Others suggested that mitigations should be considered at both device-level and organisation-level, to provide a robust approach.

Several responses noted that early guidance and ongoing engagement were needed before Government should finalise outcomes in relation to grid stability risk mitigations.

Government response

Government expects our proposed grid stability outcomes to inform the next phase of ESA standards development. However, it is recognised that ongoing input from National Grid ESO and Distribution Network Operators will be needed to help ensure grid stability mitigations are appropriate and reflect the evolving risk profile, considering factors such as diversity of ESAs and service providers, and resilience of the network to grid stability risks. As such, the 'development' phase governance arrangements, that have already been established via set of technical working groups, alongside the transition and delivery governance phases as proposed in the consultation, will embed National Grid ESO and network companies' participation in the development of policy and technical frameworks on grid stability.

In addition, we acknowledge that close co-ordination between the development of DSR licensing requirements and ESA requirements will promote a holistic approach to grid stability mitigation. Government will also consider how future grid stability mitigations for ESAs will interact with mitigations already in place (such as for EV charge points).

Energy smart appliances: Technical frameworks

Within this chapter of the consultation, we set out the technical frameworks - such as requirements, standards and systems - needed to deliver the outcomes proposed in the prior chapter. It included the following 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 achieve 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.*

Data interoperability

Time of-use tariffs

Question 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?

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

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

The consultation set out proposals to require energy suppliers, through an amendment to energy supplier licence conditions, to make time-of-use tariff data openly available in a common format. This intends to enable ESAs and their associated systems to access time-of-use tariff data over the internet, removing technical barriers to integrating time-of-use tariffs with ESAs. Given its existing role in data standardisation for smart metering, the Smart Energy Code was proposed as appropriate governance to develop these arrangements.

Summary of responses

Overall, there was strong support across all stakeholder groups on the need to intervene to deliver greater interoperability of time-of-use tariff data. This recognised the benefits of improved interoperability in enabling integration between ESAs and tariffs, and the barriers that have prevented this integration to date.

However, there were concerns raised around proposals to focus on interoperability of 'public' tariff data (i.e. data on all the tariffs in use by a supplier, without linking tariffs to individual consumers) rather than interoperability of ‘personal’ tariff data (i.e. the specific tariff of an individual consumer, associated to that consumer’s energy supplier account. Some stakeholders noted that this approach relied on consumers being able to remember or identify their tariff correctly, and raised concerns about how easily and accurately therefore a consumer could provide this information. Others raised concerns regarding how change-of-tariff or change-of-supplier use-cases would be accommodated. Several stakeholders argued that a solution to deliver ‘personal’ tariff data interoperability – whereby a consumer provides consent to a third party to obtain their individual tariff information from their supplier - would be more effective. This could be achieved either after or instead of a solution for ‘public’ tariff data interoperability.

Other challenges posed in responses included potential constraints to innovation from an approach established in regulation, and around determining the potential scope of tariffs to be included in such a solution. Some questions raised in responses related to how this solution might align to other technologies in use in the energy sector, such as smart metering.

With regard to governance, there were mixed views regarding the proposal to use the Smart Energy Code (SEC) governance to deliver these solutions. Whilst 25 stakeholders agreed that the SEC was appropriate, 14 stakeholders highlighted limitations with the SEC, such as pace of delivery and limited synergies in scope or capabilities, and some argued that the Retail Energy Code (REC) or Balancing and Settlement Code (BSC) could be more suitable.

Most respondents proposed requirements on ESAs themselves to be interoperable with time-of-use tariffs are not needed to deliver interoperability of time-of-use tariffs. Most respondents were content that making tariffs available in a common format was sufficient to deliver government’s intended outcomes, and that additional requirements prescribing how ESAs integrated with tariffs were not required as there would be sufficient commercial incentives to use the data in any event.

Government response

Given the strong consensus regarding the case for intervention, Government will intervene to deliver interoperability of time-of-use tariff data. However, Government recognises the challenges relating to the proposed approach, and believes further work is required to develop a solution that delivers the policy objective. As such, further policy development will also consider solution options that enable interoperability of ‘personal’ tariff data, whereby consumers may provide consent for their tariff data to be shared with third parties. These options will be considered alongside solutions for interoperability of ‘public’ tariff data, widening the potential scope of options compared to the initial consultation position. Evaluation of these options will consider impact to different stakeholder groups, implementation timelines and potential data privacy/cyber security risks. It will also consider interactions with other initiatives to promote interoperability of consumer energy data, including those set out in the Government’s response to the Energy Digitalisation Taskforce report.

Whilst changing the options in scope of policy development will not impact immediate timelines, we will need to consider the delivery timescales of different approaches when determining the preferred solution. Options evaluation will need to consider potential data privacy and cyber security considerations from different approaches, to ensure that consumer data is sufficiently protected. Government has procured support from an external consultancy to support with solution option development and evaluation, considering impacts on consumers, energy suppliers and users of tariff data.

In addition, future consultation will consider different governance solutions, including the SEC, REC and BSC. This recognises that further development of the technical solution will be required before identifying an appropriate governance solution. Government expects to consult on the detail of these technical and governance proposals for time-of-use tariff data interoperability later in 2023. In advance of this consultation concluding, we expect the Government to work closely with industry working groups to progress solution design further.

Government does not expect to place regulatory requirements on ESAs to require interoperability with time-of-use tariffs at this point in time. We maintain the view that delivering interoperability of tariff data will be sufficient to deliver our intended policy outcome, although this may be revisited after implementation of the eventual solution.

Other ‘Incentive’ Data

Question 13: Should Government consider standardisation by other types of ‘incentive data’ used by ESAs for DSR? Please consider what types of data and how they could be standardised.

In the consultation, examples of other types of data used by ESAs for DSR that could be standardised were highlighted as carbon intensity, wholesale energy costs or network charges.

Summary of responses

In response to the question, there was a consensus to tackling this at a later stage once a solution for time-of-use tariffs was better established. Whilst there was some support for adding carbon-based incentives to any next steps on time-of-use tariffs, many noted carbon intensity data was already available from National Grid ESO[10].

Government response

Given this feedback, the Government will not take forward any specific plans to further standardise other ‘incentive’ data used by ESAs for DSR. Relevant work on data and digitalisation work, including Net Zero Innovation Portfolio (NZIP) projects,[11] will continue to provide further evidence for data standardisation needs in this area.

[10] https://www.carbonintensity.org.uk/

[11] NZIP Flexibility Innovation Programme

Energy Smart Appliance standards

This section proposed that ESA standards would be needed to deliver secure, interoperable ESAs at scale. It established proposals regarding the regulatory approach, technical approach, scope, and delivery approach of ESA standards in the future.

Adoption

Question 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.

The consultation considered the approach to promote the adoption of ESA standards at scale, in order to deliver the benefits of interoperability, cyber security, grid stability and data privacy. Government proposed that regulation will be required to encourage adoption at scale and sought views on two high-level options for a future regulatory approach: 'outcome-based regulatory requirements' and 'presumption of conformity' through approved standards (Option 1), or mandated standards (Option 2).

Summary of responses

A significant majority of responses agreed with the need for Government regulation to drive the adoption of ESA standards at scale, recognising that a voluntary approach to standards is unlikely to drive adoption and the desired benefits. The very small minority of respondents who argued that regulation wasn't needed cited the risks of constraining the market too early and limiting innovation.

Considering the two options, 23 respondents opted for Option 1 ('approved standards'), with this option particularly favoured by ESA manufacturers. Those who preferred this option highlighted the benefits of accommodating more innovation, flexibility and international alignment, whilst mitigating the risks of mandating a standard too early. Many respondents argued that under this model, manufacturers would gravitate towards a 'de facto' single standard in any case.

Those who preferred a mandated approach, 13 respondents, noted the increased certainty for industry and consumers, and the greater confidence that policy outcomes are being delivered. These respondents also had concerns with an 'outcomes focused' approach, in that it may fragment industry efforts to develop standards, or that it may lead to a greater risk of poor consumer or energy system outcomes. Alternatively, some argued that different approaches should be taken for different interfaces[12]. Some argued that the approach could evolve over time – with some respondents initially prioritising increased certainty, and others initially

[12] For example, some respondents proposed a different approach should be taken for local and remote interfaces. Others proposed different approaches for interfaces between the ESA and the Customer Energy Manager (as described in PAS 1878), compared to the Customer Energy Manager and the DSRSP.

prioritising reduced barriers to innovation. Finally, 8 respondents did not specify a preferred option.

Government response

Government will establish regulation to promote adoption of ESA standards. This recognises the barriers to standards adoption which are unlikely to be overcome without government intervention.

Government is committed to the development of a single standard that can be used market-wide. Our ambition is that this standard should accommodate innovation in technology and business models, be compatible with other standards for interfaces where interoperability will not be required, and enable international alignment where desirable. We anticipate that this can be achieved through only standardising the minimum functionality required to deliver policy objectives and accommodating a range of different implementations for different business models and product types. In addition, we expect making the standard ‘open’ and aligned to international standards (where possible) will also support these ambitions.

Following further development of this standard, Government will consult further with industry on the regulatory approach, considering the options set out in this consultation in further detail. This will consider any further standardisation efforts within the sector, and potential opportunities to promote greater international alignment.

Proposed Standards

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

In the consultation, Government proposed to use a standard based on PAS 1878 in the future regulation of ESAs. This recognised alignment of PAS 1878 to Government’s policy objectives, alignment to emerging international standards, and the industry input provided during its development. However, the consultation also noted that PAS 1878 would require further development before being adopted at scale, following the Interoperable Demand-Side Response (IDSR) innovation programme, cyber security risk assessment and further industry input.

Summary of responses

Of 54 respondents, 36 agreed that a standard based on PAS 1878 should be used in the future regulation of ESAs, with 5 respondents disagreeing and 13 taking a neutral view. Of those who supported this approach, most acknowledged that there had been input provided during its development from different stakeholder groups, and the need for alignment with wider Government policy objectives. Furthermore, some respondents noted that there were no preferable alternatives at present.

However, many respondents proposed that further testing, demonstration, and development of PAS 1878 would be needed before it could be deployed at scale. In practice, some of the proposed changes could be incremental, whereas others could be more fundamental.

Notwithstanding the challenges and the above mentioned suggestions, many respondents still held the view that PAS 1878 is an appropriate starting point.

Government response

Government will use a standard based on PAS 1878 in the future regulation of ESAs. In practice, this means that Government will continue to support the development of PAS 1878, through facilitating a next phase of standards development and supporting development of prototypes through the IDSR innovation programme which commenced in December 2022.[13]

However, Government also recognises that the next phase of standards development will continue to be industry-led. This process will therefore need to accommodate industry proposing changes for consideration and assessment against policy objectives by different stakeholder groups. Whilst some of these changes to PAS 1878 may be incremental, it is recognised that some may be more fundamental. The “development phase” of implementation governance arrangements via use of technical working groups will aim to build industry consensus around these potential changes ahead of the next phase of standards development commencing in late 2023.

ESAs in Scope

Question 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.

In the consultation, the Government proposed that future regulation relating to ESA standards should apply to private EV charge points, heat pumps, storage heaters, heat batteries and batteries.

Summary of responses

A significant majority of respondents agreed with the 5 ESA types the Government proposed, and very few respondents argued for these ESAs to not be in scope. However, some respondents did argue that further ESAs should be in scope, either in the initial requirements or further in the future. Other ESAs which were suggested included water heaters/cylinders, hybrid heating systems, air conditioning, wet/cold appliances, EVs and secondary controls. Reasons provided included flexibility potential, scale of adoption, or risk of unintended consequences from excluding certain appliance types. Some respondents proposed for an

[13] https://www.gov.uk/government/collections/interoperable-demand-side-response-programme

appliance power consumption threshold to be used to determine what appliances should be in scope.

Government response

Government will take forward proposals to establish regulatory requirements for EV charge points (building on those established in the 2021 Electric Vehicle (Smart Charging) Regulations), heat pumps, storage heaters, heat batteries and domestic-scale batteries to use ESA standards. However, Government does anticipate that these regulations could be applied to other ESAs in the future, as the market evolves. As such, future regulatory and technical frameworks will be designed to be able to accommodate new ESAs over time.

Future policy and standards development will consider the role of Home Energy Management Systems (HEMS) – and other similar secondary controls – in the regulatory and technical frameworks, to support implementations that accommodate the delivery of policy outcomes through using HEMS in combination with other appliances. This recognises the significant role HEMS may play in the future smart home ecosystem.

In addition, Government will work with industry to examine the significance of EVs themselves, given the dependencies between EVs and EV charge points in the delivery of DSR services and their potential impact on interoperability and security. This also recognises the growing role of EVs in providing smart charging functionality.

Delivery Approach

Question 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.

The consultation proposed that industry should play a leading role in the development of an ESA standard, whilst recognising the important roles of government and the regulator in standards development. It highlighted the need for an independent (e.g., sector- and technology-neutral), experienced, primarily UK-based entity to coordinate activities across the different organisations involved. Government sought views on two possible options: British Standards Institution (BSI), or a special-purpose industry group.

Summary of responses

Responses were mixed to this question; 11 respondents opted for BSI, 9 respondents chose the industry group, 5 respondents had no preference and 7 respondents proposed a “hybrid approach” in which the coordination is split across BSI and an industry group.

The respondents that chose BSI commented on its independence, neutrality, experience and connections to international standards groups. Those who preferred an industry group referred to the ability of such a group to better track developments in technology and business models in the ESA market.

Government response

Government maintains the view that industry will have an essential role in the next phase of standards development, to determine the best approach to meeting policy outcomes. However, Government also takes the view that a neutral facilitator will be required, to facilitate consensus, coordinate the standardisation process and ensure alignment with other standards. As the UK Standards Body, BSI is well-suited to take this role. Furthermore, Government anticipates that governance arrangements that do not use an established facilitator are unlikely to be established in the time required.

As such, Government expects to establish an industry-led and BSI-co-ordinated approach to the next phase of standards development, with BSI ensuring all stakeholder groups are appropriately represented. Government will work with industry technical working groups in the first half of 2023 to design the detailed standards governance approach, to ensure the approach meets industry needs, focuses on the greatest areas of benefit and represents best-practice.

Government expects the next phase of standards development to start towards the end of 2023. This work will begin after the completion of cyber security risk assessments, progress of the IDSR innovation programme and the mobilisation of a standards governance approach for this phase.

Government recognises the importance of international alignment with ESA standards, to remove barriers to participation in international markets and, in turn, reducing cost and promoting consumer choice. In practice, greater international alignment can be achieved through ensuring standards are internationally compatible, promoting adoption of UK and international standards, and sharing best practice with overseas governments, regulators and standards bodies. Whilst BSI will support alignment of ESA standards with international standards bodies, further international engagement will be needed to enable the benefits of internationalisation. Government will continue to collaborate with overseas government officials, and consider how international alignment can be facilitated through the implementation governance arrangements discussed in the following chapter.

Minimum ESA Requirements

Government consulted stakeholders on setting minimum requirements for heat pumps, storage heaters, heat batteries and batteries in the shorter term before implementation of enduring ESA standards. Specifically, the consultation proposed to mandate a randomised delay for ESAs to mitigate risks of ESAs changing load in synchrony, seeking views on how this could be implemented and any alternative mitigations. The consultation proposed minimum device-level cyber security requirements beyond those proposed in the Product Security and Telecommunications Infrastructure Bill (PSTI), using the ETSI 303 645 standard.

Grid Stability

Question 18: Should Government mandate a randomised delay for ESAs, including heat pumps, storage heaters, heat batteries and electric batteries, to mitigate against risks to grid stability, in advance of longer-term ESA standards?

Summary of responses

There was not a clear consensus in the responses received: 24 stakeholders agreed that a randomised delay should be implemented, whilst 14 were opposed, and 18 respondents did not indicate a clear view.

There was a general recognition amongst respondents that action was needed to address grid stability issues. Few stakeholders provided evidence to support the introduction of a randomised delay, and no Distribution Network Operators responded to this question. National Grid ESO supported a randomised delay but recognised that a more sophisticated solution will be needed in the future, potentially involving multiple approaches at device and system level as the volumes of consumer flexibility increases.

Stakeholders raised concerns about unintended consequences from randomised delay, particularly for the consumer experience. This was particularly the case with heat devices where many stakeholders considered a delay might be less acceptable to consumers. Furthermore, many stakeholders recommended that it might not be in the best interests of consumers for Government to apply a blanket approach, as not all device responses are the same and may have different characteristics. There were other responses which highlighted the potential impact on consumers earning value from time-of-use tariffs.

Some stakeholders (including National Grid ESO) proposed that randomised delay should not be considered a long-term solution to synchronised changes in load as flexibility volumes increase, even though it might be suitable as a short-term mitigation.

Government response

Government is committed to mitigating risks to grid stability before they materialise. As such, government will continue to work closely with National Grid ESO, DNOs and industry to understand the risks to grid stability and the required mitigations, throughout all stages of governance.

However, Government is considering whether mitigations to the risk of synchronised response from heating appliances and batteries are required now, in advance of longer-term ESA standards. Our thinking will be informed by the number of appliances expected to be installed in this period, the scenarios that could lead to synchronisation, and the resilience of the energy system to these risks. Given the challenges raised by stakeholders to the proposed approach, Government will work with stakeholders to further consider the case for intervention and the appropriate mitigation. We anticipate further consultation later this year.

As is stated elsewhere in this consultation response, Government will also continue to promote grid stability through enduring ESA standards and licensing of DSRSPs, and continued enforcement of the Electric Vehicles (Smart Charge Points) Regulations.

Cyber Security

Question 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?

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

Summary of responses

From the 53 responses received regarding the need for minimum cyber security requirements, the majority (38) were in favour of introducing minimum device-level requirements to protect consumers. 15 respondents held a neutral position, and no respondents disagreed. Some respondents pointed out that installing smart heating appliances ahead of cyber security requirements being in place could cause cyber security risks into the 2040s, due to their average life span.

Several respondents made the point that security requirements should be considered on a risk level rather than by appliance type and that requirements should apply to all ESAs capable of being remotely switched above a given threshold load based on the likely grid impact of mass switching. Respondents proposed that requirements should be principle-based and sufficiently flexible to enable market-led solutions and not prohibit innovation.

From the 41 responses received regarding the role of ETSI 303 645, the majority (27) agreed that ETSI 303 645 is an appropriate standard. 12 respondents held a neutral position, and 2 respondents disagreed. Those who agreed noted it would provide flexibility for consumers to innovate and implement security solutions and that it strikes the right balance as an outcomes-based standard that aligns with international standards.

Government response

Government intends to proceed with minimum cyber security requirements for heat pumps, storage heaters, heat batteries and domestic-scale batteries, in advance of developing ESA standards for the longer-term. We consider such requirements to be an important initial step in mitigating cyber security risks to protect consumers, the energy system infrastructure and maintain confidence in low carbon consumer technologies. There is a clear need for such requirements ahead of any enduring ESA standard solution being in place, given the likely high proliferation of certain ESAs by the mid-2020s and the typical lifespan of these devices. The draft legislation and implementation approach will be subject to further consultation in 2023.

At this stage, using ETSI 303 645 as the basis of these requirements remains our lead option, ahead of the development of more enduring standards for ESAs. Implementation of our minimum cyber security requirements are expected in the mid-2020s (2026 - 2027). This will help ensure Government have the opportunity to work with stakeholders to consider the most suitable approach to cyber security requirements prior to finalising them in legislation. Throughout this process we will engage with industry technical working groups to understand how best to manage the transition between the minimum requirements and the enduring requirements in an ESA standard.

As is the case for other proposals in the consultation, Government will consider further the role of HEMS and secondary controls in this approach, recognising the potential security implications of these devices.

Common Systems

Question 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?

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

Common, shared systems or infrastructure may be required to mitigate risks across the system as a whole. The consultation put forward initial considerations to illustrate three areas where common systems and infrastructure could be required: Public Key Infrastructure (PKI), anomaly detection and communication networks. It noted that Government does not expect to prescribe communication networks for ESAs. This section also discussed the approach to delivering common systems, if needed.

Summary of responses

Many respondents recognised that Public Key Infrastructure is an area where common systems could be required, although noted that further technical solution development will be required before determining an appropriate approach. Multiple potential solutions were proposed by respondents. Some proposed that a model with a single Root Certificate Authority, with competition between sub-Certificate Authorities, could find the appropriate balance between security and flexibility, and should be developed further. Some respondents identified risks associated with central systems, such as barriers to innovation if they are unable to respond to change, cost to system users, single points of failure and time required to implement. Some respondents proposed that existing commercially available PKIs are suitable for use in this context. Others suggested an approach that utilised a common list of ‘trusted’ Root Certificate Authorities, although some noted the potential complexity of this approach.

A wide range of considerations were put forward relating to anomaly detection, although many recognised that further development is required in this area before deciding on the approach. Some respondents recognised that the risks to grid stability from ESAs warranted a centralised, system-wide approach that may deliver a stronger mitigation than a de-centralised solution. Others noted that a single market-wide solution could be lower cost than different organisations using their own solution. However, others were concerned with the overall cost, innovation constraints and implementation timescales of a highly centralised solution, and some respondents put forward alternative mitigations.

Of those who commented on communication networks, almost all agreed with the consultation proposals to allow use of existing communications infrastructure, subject to appropriate security mitigations.

Some respondents also noted other common systems for ESAs that could promote delivery of policy objectives, noting the recommendations of the Energy Digitisation Taskforce report. Examples included a central asset register and data sharing platforms.

Of the 39 respondents who addressed the question regarding a delivery approach for common systems, only 7 opted for one of the proposed options. The remainder did not express a clear preference, noting that further detail and consultation would be needed. Specific points raised against each of the options include:

- **Option 1 (Extend DCC – the smart meter network Data Communications Company)** – Some respondents thought this would be possible but with a number of technical and regulatory hurdles to be addressed. A number of respondents raised concerns with this option, such as risks of reducing focus on existing delivery obligations, and the cost/constraints to innovation of a highly centralised model. Others raised a number of benefits, such as re-using existing capability and investment.
- **Option 2 (New licensed body)** - Several respondents agreed with reasoning for discounting Option 2. One respondent argued this could be justified if the size of body was large enough.
- **Option 3 (New central body to procure common systems)** – One respondent noted that it could allow the most tailored solution. Other respondents thought it could take too long.
- **Option 4 (Approved service providers)** – Several thought this model would be the most dynamic and supportive of innovation. Others thought it risks complexity, inefficiency and could create complexity for service providers.

More broadly, several respondents raised concerns on the cost of the system itself and costs to integrate with the system, with several suggesting that any centralisation should be avoided. Others also noted that central systems can form a common point of failure. Several respondents noted the impact on implementation times of common systems, as ESA manufacturers and DSRSPs would need further time to integrate with systems during product development and testing, in advance of products being placed on the market.

Government response

As described in the consultation document, Government is working with NCSC and industry to complete a cyber security risk assessment for ESAs and DSR, which will inform a future security architecture and any requirements for common systems. Government expects industry to input into this work through an industry working group focused on security, before determining a preferred security architecture ahead of consultation with industry. As proposed in the consultation, if common systems are required, Government does not anticipate creating a new licensed body with similar remit to the DCC.

More broadly, Government will continue to consider interactions with findings from Flexibility Innovation Programme projects, including the Automated Asset Registration (AAR) competition, for further evidence on the potential need for common systems for domestic appliances.

Energy smart appliances: Delivery frameworks

Within this chapter of the consultation, the Government set out how the technical frameworks for secure, interoperable ESAs will be delivered in practice. It sought 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.

Implementation Governance

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

The consultation proposed a phased approach to implementation governance, moving between the ‘development’, ‘transition’ and ‘delivery’ phases. In the latter two phases, Government proposed that more substantive governance arrangements will be required and put forward two options: (1) establishing a central, not-for-profit, delivery body, and (2) building on existing Smart Energy Code (SEC) governance arrangements.

Summary of responses

40 stakeholders responded to this question. Many respondents considered how governance should accommodate innovation, such as through delivering at pace, flexibility in approach and ability for simulation and testing. Others stressed the need to prioritise the consumer in a market-led approach, with interoperability included early in deployment. Others focused on the need for alignment with international standards and approaches. There was concern about how to deliver in an efficient and agile manner, aligning to the pace of change in the market. Others cited the need for cost effectiveness, accountability, independent leadership and a clear road map through the different phases of transitional governance. A common point made was that implementation governance needed to be transparent and streamlined, whilst including the right level of expertise and seniority from stakeholders.

Only 11 respondents articulated a preference between options for ‘transition’ and ‘delivery’ phase governance. Of these, Option 1 (establishing a central, not-for-profit delivery body) was favoured by 8 respondents and Option 2 (building on SEC governance arrangements) was favoured by 2 respondents. Reasons for supporting Option 1 included the benefit of a body with a singular focus on ESA governance, avoiding potential issues that may arise from using an existing body, and a greater ability to promote innovation and internationalisation. However, a small number of stakeholders raised concerns with the potential costs and complexity of establishing new governance frameworks.

Of the stakeholders who mentioned SEC, there were common concerns about the lack of synergy between SEC and the scope of a new framework, potential detrimental impacts to smart metering delivery, the ability of SEC to deliver at pace, and the scale of change required to SEC. One respondent noted that the SEC lacks the flexibility and adaptability to be used in the sector, given the fast-changing nature of the sector and the number of non-traditional players in the sector. Other stakeholders suggested that the SEC should only be used in full if the DCC is to be used, given the role of the SEC in governing the DCC's activities.

On the other hand, another respondent suggested that proceeding with SEC would be cheaper, faster and utilise existing expertise. An alternative option was suggested by one respondent, who proposed to build on existing governance arrangements from the Balancing and Settlement Code (BSC), given the potential cost and complexity of creating a new body.

Government response

By creating industry technical working groups, the Government has established the initial 'development' phase governance arrangements that will co-ordinate input between government, industry, and regulators. Further information on these working groups can be found in the "Stakeholder engagement & next steps" section of this document.

Government will continue to work with industry to consider the appropriate model for 'transition' and 'delivery' phase governance. This work will consider interdependencies with other questions relating to delivery approach, such as ESA standards, common systems and assurance schemes and cost recovery, that will be significant in determining the optimal approach. Government will consider impacts of overall cost, implementation timelines and effectiveness of different options. These further proposals will be set out in a further consultation, in advance of establishing these arrangements in full.

Demonstrating Compliance

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

Assurance

Question 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.

Question 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.

In this section, Government put forward a number of considerations relating to the assurance of products against the proposed regulations. The Government proposed the following, device-level assurance options:

- Option 1: Self-certification without testing
- Option 2: Self-certification with testing
- Option 3: Third-party certification with testing

The consultation proposed that ESAs will require a robust but proportionate approach for demonstrating compliance with cyber security requirements, potentially using third-party testing and certification. The consultation also sought views on assurance requirements for supporting systems or cloud-based platforms.

Summary of responses

Respondents proposed that assurance schemes should promote market-wide participation and a level playing field. Some raised concerns regarding the additional time and cost of third-party certification. Some respondents proposed that technical testing requirements should be designed in collaboration with industry. Some stakeholders considered that Government should consider how to ensure manufacturers and DSRSPs maintain security across the lifetime of products and services.

On preferred assurance approach, very few respondents (6) supported Option 1 (Self certification without testing), due to doubts it could deliver policy outcomes adequately. However, those who supported Option 1 noted that this option benefits from lower cost and reduced dependency on availability of testing houses. 14 respondents opted for Option 3 (Third party assurance with testing), whilst noting that it had advantages and disadvantages, offering robust assurance but with barriers such as cost and capacity constraints at testing houses. Finally, a sizeable minority of respondents (11) supported Option 2 (Self certification with testing), stating that it was a middle approach that balanced the advantages and disadvantages of the other two options. Option 3 (46) received the most support from stakeholders, followed by Option 2 (35) then Option 1 (19).

Respondents also provided views on the assurance for supporting systems including cloud based platforms. Some respondents proposed that systems interacting with critical national infrastructure should be subject to robust assurance, such as penetration testing by an independent third party.

Government response

Government's view is that Option 1 (self-certification without testing) will not provide the appropriate level of assurance that policy outcomes, such as security and interoperability, are met. As such, Government will discount Option 1 from further policy analysis. As stated in the consultation, Government will consult further on the most appropriate assurance approach for ESAs, considering testing requirements with both self-certification and third-party certification.

Labelling

Question 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?

The consultation considered whether to introduce a smart functionality labelling scheme for ESAs, citing the potential benefits for consumer engagement in smart and DSR services. The consultation also mentioned the role of an ESA label in advertising to consumers that products are meeting certain regulatory requirements, for example on interoperability or cyber. The consultation did not offer a view as to whether such a label would be mandatory or voluntary.

Summary of responses

Of the stakeholders who responded to this question, 28 agreed that a labelling scheme for ESAs would help promote consumer participation in DSR, noting that it would help improve consumer confidence. Common themes of the 4 respondents who disagreed were that they believed labelling would offer little benefits to consumers as it would be reliant on additional consumer education. Some respondents proposed that it would not be worth the effort to create a labelling scheme. Finally, 15 respondents offered a neutral position as to whether a labelling scheme would be beneficial or not.

Government response

Government recognises the importance of consumer engagement, to promote adoption of DSR and ESAs more broadly. However, Government is also mindful of the complexity and cost of implementing a labelling scheme to industry, regulators and Government. In particular, a ‘smart functionality’ label, that indicates to consumers the level of smart functionality of an ESA, may not provide incremental benefits to consumers, when introduced alongside market-wide regulation to promote smart technologies. Furthermore, the impact and benefit of such a label will depend on the design of the standards for ESA interoperability.

As such, Government does not have plans to progress the development of a smart functionality label at this current time. However, we will revisit this question once ESA standards have been further developed. We will continue to explore whether a label for compliance purposes is beneficial. As committed to in the 2021 Smart Systems and Flexibility Plan, the Government will continue to consider the merits of introducing a separate 'smart readiness indicator' (potentially within Energy Performance Certificates) for assessing how optimised a building is for smart technologies.

Cost Recovery

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

The consultation set out the need to establish processes to recover the costs associated with the delivery of the ESA proposals. Examples of how such costs could be recovered are provided, such as via ESA manufacturers by passing the costs back onto the sale price of ESAs, via DSRSPs through services they provide to their customers as well as through energy suppliers via energy bills, and Government via general taxation. The consultation sets out how costs will change over the course of governance arrangements for the ESA proposals, noting that Government will fund ‘development’ stage governance, with costs transitioning to industry during the transition and delivery phase.

Summary of responses

The majority of respondents generally agreed that the Government should use its own resources for the initial stage of the ESA governance arrangements, and over the longer term spread the costs across a wider group of actors. The majority of responses highlighted that the cost recovery process should ensure that those that benefit the most from the proposed requirements, incur most of the immediate cost.

A number of responses highlighted concerns that smaller organisations could be disincentivised from participating in the market if costs are too high, or that costs passed on via ESAs or DSR services could disincentivise uptake. A number of responses highlighted the benefits that network operators get from increased flexibility, and the subsequent rationale for them to bear costs. Some responses raised concerns about recovering costs from consumers who do not directly benefit from flexibility.

Government response

As noted earlier in this chapter, Government will consult further on implementation governance, which will also consider how costs should be recovered. These final proposals will be set out prior to Government laying secondary legalisation and establishing any new capabilities.

Mandating Smart Functionality

Within this chapter of the consultation, the Government set outs proposals for mandating that electric heating appliances have smart functionality. The consultation asked stakeholders for their views on these proposals and sought input on the proposed scope, implementation date, and the definition of smart functionality for the purpose of the mandate. We also sought views on extending the mandate to other appliances, including domestic-scale electric battery systems.

Appliances in scope of the mandate

Question 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.

Summary of responses

We received 46 responses to this question. An overwhelming majority agreed that hydronic heat pumps, electric storage heaters, and heat batteries should be mandated to have minimum smart functionality. Of those who agreed, the majority said it should also be extended to include further appliances.

Those in favour of extending the mandate to other appliances suggested including hot water storage, hybrid heat pumps, air-to-air heat pumps and domestic hot water heat pumps. Under a third of respondents suggested that it should be extended to all electric heating appliances and/or that the mandate should be based on an appliance's electrical demand, as opposed to thermal capacity, to capture all heating/cooling appliances with a high electrical load.

Eight respondents highlighted the benefit of applying the mandate to the broader system, for example to the Home Energy Management System (HEMS), or to smart heating controllers, instead of at the appliance level. Some noted that the mandate should be applied retrospectively to existing heating appliances, for example by requiring that a smart controller be fitted onto to non-smart appliances.

Question 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?

Summary of responses

We received 31 responses to this question. Some respondents reiterated views they shared in responses to Question 28.

Under a third of respondents said domestic hot water storage should be included in the future and that the mandate should be extended to capture all electric appliances with a curtailable load, such as Heating, Ventilation, and Air Conditioning (HVAC) and white goods. One stakeholder suggested that manufacturers of appliances such as domestic hot water storage should have the option to comply with standards voluntarily.

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

Summary of responses

We received 36 responses to this question. A significant majority of respondents indicated that domestic-scale electric battery systems should be in scope of the mandate, and some commented that they should be subject to an interoperability standard that ensures they can work alongside other appliances in the home, for example a heat pump. Two stakeholders suggested that solar PV sold with batteries should have to meet the mandate and the same interoperability standard.

Only two stakeholders disagreed with including domestic-scale electric battery systems. This was on the basis that most domestic batteries are already 'smart-enabled', and they were not convinced of the merits of additional regulation prior to the development of a fuller standard for interoperability, which is expected in the mid-late 2020s.

With regard to other appliances, there were continued calls for the inclusion of domestic hot water storage and other domestic appliances which put a curtailable load on the grid, including air conditioning and white goods.

Government response – Questions 28, 29, 34

We intend to mandate that all hydronic heat pumps, storage heaters, and heat batteries up to 45kWh rated thermal capacity must have smart functionality.

We recognise the points made by industry with regard to other appliances that should be in scope and are open to a potential extension of the mandate. With regards to hybrid heat pumps, in the consultation we proposed that the smart mandate apply to the hydronic heat pump element of any hybrid system. Taking into account the feedback from stakeholders, further consideration will be given to determine if and how the mandate should apply to hybrid heat pump systems. We will consult further on this, as well as any proposals to bring further electric heating appliances into scope, before laying secondary legislation.

We note that there was strong appetite for extending the smart mandate to domestic-scale electric battery systems. We will ensure that such systems which are smart meet the minimum ESA standards we intend to introduce. However, we do not propose banning the sale of non-smart domestic batteries at this time. This is on the grounds that the majority of batteries in the market are already able to adjust their use of energy in response to signals, meaning that a smart 'mandate' might add little benefit; and that there may be use-cases where non-smart batteries fill a genuine consumer need, for instance in off-grid homes. However, we will keep this position under review.

We also acknowledge the case that has been made for applying the mandate to the broader system, such as smart controls, as opposed to applying it on specific devices. We intend to progress with the proposed approach of mandating smart for specific appliances, rather than the building as a whole. However, as set out in the proposed definition, we intend to allow for the smart functionality of an appliance to be provided by an add on module, which could potentially be a third-party smart control. We will use future consultations to explore how organisations will demonstrate compliance with the mandate when delivering smartness through a third-party control system.

Definition of a smart heating appliance

Question 31: Do you agree with the proposed definition and approach to delivering smart functionality for electric heating appliances?

In the consultation we proposed to define a smart electric heating appliance as an electric heating appliance which is communications-enabled and capable of responding automatically to incentive signals (such as price) and/or other more direct control signals by shifting or modulating its electricity consumption. This smart functionality can be embedded in the appliance or provided by an add on module.

Summary of responses

We received 39 responses to this question. The majority of respondents broadly agreed with the proposed definition. Some agreed on the basis that the high-level definition allowed for innovation and flexibility whilst others thought it could act as a starting point but required further development. Some respondents suggested small edits or additions to the definition, with one respondent helpfully noting that the wording on 'more direct control signals' deviates from the PAS 1878 definition.

Some respondents suggested additional requirements that should be placed on smart appliances. This included requirements for a consumer interface; performance monitoring capabilities; and for the appliance to externally communicate information such as temperature or location of the home.

Five respondents disagreed with the definition. The majority of these disagreed on the basis that requirements should be placed on the system, for example the HEMS, rather than the appliance.

Government response

The policy intent of the smart mandate is to set minimum requirements which enable DSR, without limiting innovation. On that basis we intend to proceed with the proposed definition of a smart electric heating appliance, with a small edit to more closely align with the definition of an ESA in PAS 1878 as follows: an electric heating appliance which is communications-enabled and able to respond automatically to price and/or other signals by shifting or modulating its electricity consumption. To note, this is a working definition to support the development of the regulations, and not necessarily the exact definition that may be used in future legislation. We also intend to proceed with our approach of not specifying whether the smart functionality must be embedded or delivered via an add-on module, to provide industry with the flexibility to decide how to meet the mandate.

We note the suggestions made by several respondents on the additional requirements that should be placed on smart electric heating appliances. We will further consider if and what additional requirements may be appropriate. Any additional requirements will be subject to further consultation.

Timing of Implementation

Question 32: Do you agree with the proposal to implement the smart heating mandate from 2025?

Summary of responses

We received 44 responses to this question. The majority of respondents agreed with the proposed implementation date, with several calling for introduction as soon as possible to ensure consumers are not locked out of DSR and to avoid significant uncurtailable load being placed on the grid.

Under a third of respondents disagreed with the proposed implementation date. Five stakeholders proposed that the date should be brought forward, whilst three thought it should be pushed back to allow enough time for compliant products to be developed and manufactured. Some respondents felt it was not possible to answer the question without more detailed specifications of the requirements for a smart electric heating appliance.

Several respondents noted the need for the timeline to account for agreement on standards and development of compliant products, with several flagging that the specific guidance or specifications need to be agreed and published well in advance of the regulations coming into force.

More broadly, three respondents raised concerns with the proposed approach to phasing the ESA requirements, noting that this could cause issues for both manufacturers and consumers.

Under a third of respondents suggested other vehicles for driving the uptake of smart electric heating appliances. These include an uplift for smartness in the market mechanism for low carbon heat, an earlier introduction of the mandate in Scotland to align with the introduction of Scotland’s New Build Heat Standard, and contingency measures such as retrofitting non-smart heat pumps with smart controls if there are delays in implementing the mandate.

Government response

We share the view expressed by many respondents that implementing the smart mandate as soon as possible is important to unlocking benefits for consumers and the grid. However, this must be balanced against the need for timeframes that are deliverable by industry and do not create a barrier to the Government’s ambition to deploy 600,000 heat pumps a year by 2028. We recognise the points raised by stakeholders about the need to account for product development timelines, and the importance of learning lessons from the implementation of the EV smart charge point mandate. We also recognise concerns raised by some around the burden that the proposed phased approach to implementation of the requirements may place on industry.

Therefore, we intend to combine the first phase of ESA regulations, as set out in the chapter on ‘Minimum ESA Requirements’, with the smart mandate. Ahead of implementation we intend to consult again, later this year, on the detail of the requirements for smart heating appliances, before laying secondary legislation. There will follow an implementation period, to allow time for industry to develop compliant products before any enforcement action is undertaken.

With this in mind, and considering the feedback, our ambition is for the smart mandate and minimum ESA regulations to be enforced in the mid-2020s (2026-27). We will work closely with stakeholders to agree a detailed implementation plan that ensures we are working towards an ambitious but deliverable timeline.

We recognise and encourage the positive progress that industry is already making towards delivering electric heating appliances with smart functionality as standard and will consider how we can support industry to accelerate the deployment of smart heating in the period prior to the mandate’s implementation. This includes progressing work to act on our commitment in the Smart Systems and Flexibility Plan to ensure flexibility is considered across energy efficiency and heat policies. This includes assessing the role of smart technologies in Building Regulations and working with industry to incorporate flexibility and smart technologies into the Standard Assessment Procedure (SAP, the national methodology used to assess the energy performance of a home).

Longer term approach

Question 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 customers, in terms of upfront costs or otherwise? What further action is needed to ensure all groups can benefit from smart heating?

Summary of responses

We received 38 responses to this question. Nine respondents said that the mandate would add zero, or very little, cost to the upfront cost of electric heating appliances in scope. This group emphasised the long-term benefits of smart appliances and two stakeholders argued that they would outweigh any additional cost.

The majority of respondents noted the importance of protecting low-income and vulnerable consumers against the impact of any additional cost, and two stakeholders stressed the importance of smart controls being developed with the needs of these groups in mind. Several respondents highlighted that these groups have the most to gain from smart appliances but are least able to afford or engage with the benefits they bring, for example because of tariff availability, poor insulation, or computer literacy.

Some respondents highlighted that the main barrier to uptake is the high upfront cost of low-carbon technologies, rather than the additional cost of making them smart. Therefore, the mandate might only benefit consumers who are able to afford the relevant appliances.

There were a range of suggestions on how to support low-income and vulnerable groups through the transition to the electrification of heat. This includes providing tailored advice and engagement on the benefits of smart heating to landlords, consumers, and housing associations, targeted flexibility initiatives, and further support for smart appliances and energy efficiency through government schemes.

Question 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?

Summary of responses

We received 35 responses to this question. Overall, the majority of respondents acknowledged the importance of building inertia and thermal storage for maximising the flexibility from heat pumps, whilst maintaining comfort.

Over a third of respondents disagreed with the need to mandate a minimum level of storage, whilst under a third agreed with the proposal. Of those who disagreed, the majority said there should be enough flexibility in a well-designed heating system and from the inertia of the building, without needing additional requirements. Almost half were concerned that it could slow down heat pump rollout or felt it should be based on consumer choice and/or impartial advice on a home-by-home basis.

Government response – Questions 30, 33

We agree with respondents on the importance of making sure all consumers, particularly low-income and vulnerable groups, can benefit from smart heating.

The Smart Systems and Flexibility Plan set out the ambition that, in the mid-2020s, consumers of all kinds will have the opportunity to choose and benefit from smart energy products. However, we recognise that low-income and vulnerable groups may face barriers to entry, and that they need the knowledge and resources to access smart appliances and understand how to maximise their benefits.

We will continue to explore additional measures that may be needed to support access to, and use of, smart appliances. This includes further research such as the forthcoming project on

Inclusive Smart Solutions, which will seek to identify innovation needs to help low income and vulnerable consumers participate in a smart and flexible energy system.

We also acknowledge the important role that energy efficiency will play in enabling consumers to use their electric heating appliance flexibly and reduce their energy bills. That is why the Government has committed to spending £6.6 billion over this Parliament on low-carbon heating and energy efficiency and a further £6 billion between 2025 – 2028, which will align with the implementation of the smart mandate. A new £1 billion ECO+ scheme has been established to deliver energy efficiency improvements and extend support to the least energy-efficient homes and vulnerable groups. There is also targeted support via the Social Housing Decarbonisation Fund and Home Upgrade Grant.

Thermal storage has a role to play in providing flexibility, in addition to the thermal fabric of the building. However, based on the feedback shared in the consultation responses, we do not think there is a case at this stage to mandate a minimum level of thermal storage.

Regulation of Organisations

Within this chapter of the consultation, the Government proposed to introduce regulatory requirements on organisations providing demand-side response to domestic and small non-domestic consumers. This was proposed to give consumers confidence to participate within the demand-side response (DSR) market, whilst ensuring both consumers and the energy system receive the benefits. Government is planning to consult in closer detail on proposals for licensing later this year and the responses below set out on what areas will be considered further.

Organisations in Scope

Question 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?

Question 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?

Government proposed that licensing scope should include those who enter into arrangements with domestic or small non-domestic consumers for the purpose of DSR. There are multiple approaches to implement a future regime – for instance Government could establish the scope of regulations with reference to consumer type and/or the Energy Smart Appliance (ESA) device.

Summary of responses

For question 35, out of 49 respondents, just over half (26) agreed that both domestic and small non-domestic customers were appropriate starting points for regulatory intervention. Some respondents diverged over whether small non-domestic consumers should be in scope. Few (5) cited Ofgem and Citizen’s Advice research that microbusinesses experience similar risks to domestic customers and that they should be included, though a few others commented that the focus should remain on domestic customers only. A few (5) requested clarification on small non-domestic definition but did not express a preference on the type of consumer that the licensing should apply to. 13 respondents were neutral with no preference expressed on the licensing scope.

10 respondents disagreed with the proposed focus, with half believing licensing should apply to all organisations providing DSR and not be limited to domestic and/or small non-domestic consumers and the others rejecting regulatory intervention.

A few respondents believed that organisations that already provide DSR services[14] to the grid could have reduced licence requirements. A couple of stakeholders expressed the view that small non-domestic organisations should be considered for exemption from licence arrangements as they tend to prefer minimum intervention in their businesses and complete control of their appliances.

For question 36, out of 38 respondents, half (19) felt that a licensing scheme should be linked to providers of services, nine felt that it should be linked to the size of the customer portfolio, and the remainder expressed other views. There was a theme from respondents that licensing should focus on service providers who contract with consumers or who are consumer-facing organisations. Some stated that licensing should focus on providers posing significant grid stability risks, with a proportionate threshold above which licences would be required.

It was felt that a licensing scheme should be flexible to a range of organisations, with a few respondents suggesting licensing should be linked to activities rather than specific products. A few participants added that licence conditions should be high level and not be prescriptive for easier implementation and to avoid constricting the market early. Some viewed that licensing should be 'device agnostic', with a couple saying that if devices were to be specified, then essential devices such as smart heating appliances should be prioritised.

Government response

Government expects that initially, future proposals on licencing will focus on ensuring domestic and small non-domestic consumers are protected in their arrangements with organisations providing DSR. Extension of the scope of licensing to non-domestic consumers and the precise definition of 'small non-domestic consumers' for the purposes of the licence will be subject to further consultation in 2023. Government will consider the particular risks to microbusinesses in DSR arrangements in further policy development.

Government will consider the scope of the licensing regime for devices not currently covered by the proposed ESA regulations. This position will be subject to further consultation in 2023.

Design principles

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

In the consultation, Government proposed several design principles to create a future regulatory framework. These principles would guide policy development, but not be a hard constraint on future design. The principles are listed below:

- Scalable and proportionate – regulatory requirements and other aspects of the framework should be suitable for organisations with different sizes and risks posed.

[14] https://www.nationalgrideso.com/industry-information/balancing-services/demand-side-response-dsr (accessed 24/11/2022)

- 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.
- Support market access and enable innovation – unnecessary barriers to new entrants obtaining a licence should be avoided.

Summary of responses

Out of 33 respondents a significant majority (25) broadly supported the design principles, with ten of those supportive respondents also suggesting further principles including ‘customer-centricity’, ‘accountability/transparency’, and ‘energy stability’. 5 were neutral, and a few (3) respondents were against the design principles outlined on the basis that regulation was inappropriate for DSR. Other suggestions included ‘clarity of regulation’, ‘regular review of licencing’, ‘enforceability’ and being ‘device agnostic’.

Government response

Government will continue with the published design principles as they are during the policy design phase. The suggested additions are welcomed and are important aspects to consider within a future licensing scheme, but we do not see a strong case for adding them to the design principles at this stage. Government will continue the policy design phase for policy options for consultation in 2023, with the suggested additional principles feeding in during the process.

Proportionality

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

In the consultation, Government acknowledged that organisational requirements need to be flexible and proportionate, to ensure that organisations are not subject to unreasonable barriers to entry or operation in the sector, and incentives to innovation are maintained.

Summary of responses

Out of 34 responses, a significant majority (25) were in favour of proportional approach within a future licensing framework. Respondents felt that a regime needs to be balanced between fostering a competitive market whilst ensuring safety, security and/or consistency across the energy system, and should be “lighter-touch” for small entrants, proportional to the risks posed. A significant number of responses believed there should be a minimum set of obligations.

Some of these respondents who were in favour of proportionality, said it should be supported by a clear and simple licensing scale, with a couple of respondents suggesting proportionality could be focused on the rigour of compliance and monitoring rather than on licence obligations.

A minority of respondents (4) felt that there needs to be consideration of whether there needs to be minimum conditions which would apply to all licensees, in recognition that there could be risks presented to all, despite their size and load. Respondents who were concerned about proportionality either believed a licensing regime was inappropriate, or that standards should be universal across all organisations, rather than containing scalable requirements.

Government response

Government will look to find a proportional balance between mitigating risks to consumers and grid stability, and avoiding introducing barriers to market incomers and innovation. This could include 'tiering' licensing where conditions are expanded for larger organisations who would pose higher risk, and whether there should be a set of minimum licencing conditions which should apply to all participants. How proportionality will be achieved in a licensing regime will be consulted on in more detail in a consultation later in 2023.

Proposed Contents of Licences

In the consultation, Government set out that the existing electricity supply licence conditions provide additional protections for consumers entering into contracts/agreements with energy suppliers beyond existing consumer protection law. Government outlined a number of additional protections that may be required, especially as DSR becomes more popular across a range of specific areas.

Consumer Protection and Data Privacy

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

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

Summary of responses

For question 39, out of 34 participants, a majority (18) agreed additional protections should be included within a future regulatory regime, with 9 disagreeing. The majority agreed that the additional protections proposed were sensible, with suggested consumer protections including:

- Consumers having control over their own data.
- Need to ensure DSRs act in the consumer interest.
- Need for a code of practice.
- Concerns about digital exclusion for some consumers.

- Insurance if DSR activities leads to damage of assets.
- Concerns about DSR organisation insolvency and them not being 'fit and proper'.
- Need for consumer access to accurate and timely data (e.g., billing), and being able to compare DSR products to make an informed choice.

Most of those who disagreed argued that existing consumer protections were sufficient and therefore nothing further was needed, though the Government should review this as the market developed. Others remarked adding additional layers of regulation would add costs to provision of flexibility, or that they did not think licensing is the right way forward in this area.

For question 40, out of the 33 respondents, the majority (17) believed that current UK data protection law was sufficient, with nine believing additional protection was needed. Those who believed current UK data protection law is sufficient thought additional data protection requirements would likely increase costs and stifle innovation, and that the consent process is complex and expensive. Of the 9 who believed additional measures should be introduced, five thought this should be implemented along similar lines to the Smart Metering programme to ensure consistency of practice. Neutral (7) respondents stated that additional protections should be included only where cyber security vulnerabilities are identified.

Government response

Government set out in the consultation specific areas where additional protection may be required, such as allowing a consumer to make an informed decision, being 'locked' into certain products and contracts, providing support to vulnerable consumers, redress, and managing risks around insolvency of DSR organisations. Consumer data privacy protections are also important for ensuring confidence in the sector as new products and services emerge.

Government will continue to develop policy proposals with the suggested areas in the consultation and will take forward and consider the further additional protections suggested by respondents, such as consumer control over their data, a need for a code of practice, and the need to ensure DSRSPs act in the consumer's interests. Government notes that a voluntary code of conduct, HOMEFlex, is currently being developed by industry stakeholders and will continue to engage with those involved in this.[15] The proposed consumer protection conditions will be consulted on in more detail later in 2023. Government also notes the approaches outlined in both PAS 1878 and PAS 1879 on the handling of consumers' personal data. As noted elsewhere in this document, Government is proposing device-level standards for ESAs based on PAS 1878 and so considers that many privacy and data protection risks to consumers could be addressed with the development and implementation of these device requirements. In the next stage of policy development for the licensing framework, the Government will further consider what requirements are needed on organisations to ensure consumers' data is adequately protected.

[15] HOMEFlex - https://www.flexassure.org/homeflex

Cyber Security

Question 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) Network Information Systems (NIS) measures outlined elsewhere in this consultation? Please explain your answer.

The consultation included a number of proposals that will impact the cyber security of organisations which provide DSR, but there may be organisations that are out of scope of those proposed regulations. This could include organisations that are not brought into scope of the NIS Regulations, but that could cause consumer detriment and undermine confidence in DSR were they to be compromised via a cyber-attack.

Summary of responses

Out of 25 respondents, a significant majority (18) agreed that licencing requirements would be appropriate for managing cyber security risks. Most felt that this would be an important measure to capture organisations who fall outside of NIS Regulations and provide clarity of what minimum requirements such organisations should comply with. Few respondents believed measures could be applied differently depending on risks posed by organisations. Others felt additional detail is required on the type of licence / what the licence conditions would be or how it would be worded. Five respondents disagreed, with one respondent remarking the European Telecommunications Standards Institute (ETSI) standard has already been applied and others believing risks could be managed through other commercial avenues or device targeted regulation.

Government response

Government proposes that licences should include cyber security requirements but will consider this in more depth in the context of wider cyber security provisions and policy development being taken forward as set out elsewhere in this response. Government's view is that the market alone is not an adequate driver of cyber security in the energy sector; voluntary codes are unlikely to drive the necessary level and consistency of cyber security resilience for the future. Further details of what licence conditions could be required to ensure cyber security will be reviewed as part of the next stage of policy development, with Government's updated position being set out in a consultation in 2023.

Interoperability

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?

In the consultation, Government proposed introducing licence conditions to ensure DSRSPs operate systems that avoids barriers to switching, ensure contracts don't unfairly lock consumers in, and ensure that DSRSP registration / de-registration of appliances does not compromise the appliance or consumer experience.

Summary of responses

Out of 37 participants, a significant majority (27) agreed with the principle that DSRSPs should not be able to abuse a dominant position in the market, which should remain open, competitive and encourage growth. It was noted that legislation should not discriminate against cases where DSRSPs provide additional DSR functionality beyond the minimum required. Four respondents disagreed that licence conditions were the most appropriate way to ensure organisations did not unfairly use their market position, stating that existing competition law would help achieve the proposal's aims.

Government response

Government will introduce licence conditions to prevent consumer lock-in and other anti-competitive practices, where appropriate. As with proposals on data privacy, Government notes that PAS 1878 includes provisions on a device level to enable interoperability of ESAs across different DSRSPs. Government will consider how proposed licence conditions could interact with any future technical standards for ESAs and DSRSPs based on PAS 1878. Government will also consider issues such as contractual lock-ins and how new licence conditions could interact with existing consumer law. This will be consulted on further in a 2023 consultation.

Grid Stability

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?

In the consultation, Government proposed that licence requirements on organisations would assist with realising additional benefits. These requirements would ensure organisations appropriately manage their portfolios of devices in aggregate and would emphasise the need to consider local network capacity when synchronising their managed appliances, engaging with DNOs to inform them of the amount of load they control.

Summary of responses

Out of 24 respondents, the majority (13) agreed that license conditions may be useful to mitigate risks to grid stability, with only three respondents disagreeing. Five respondents mentioned that licence conditions should be scalable depending on risk. One believed that load controllers, having a regard for distribution level constraints would be inconsistent with other electricity market participants.

Government response

There will be an element of risk to the grid presented by DSR organisations, scaled by the size of the load they control. Government will need to consider including proportional controls to mitigate these risks, whilst being mindful of introducing barriers to entry. Government will consider licence conditions to mitigate these risks presented to grid stability for consultation in 2023.

Other risks, and analysis

An Analytical Annex was published alongside the July 2022 consultation, which aimed to gather evidence to be used as part of further impact assessments that will be commissioned alongside secondary legislation on the final detail of our proposals. The consultation also asked a question regarding views on other potential risks that were not captured within the scope of the consultation.

Other risks

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?

Summary of responses

There were 26 responses to this question. The most common point made across responses was on the importance of ensuring a wide range of load control activities are captured by our proposals, with a total of 9 mentions of this within the responses. Other common points were on the need to include the manufacturing of EVs within the remit of our proposals to avoid grid stability risks, there were 4 mentions of this within the responses. There were also 4 mentions of different ways the Government could expand on grid stability requirements to better address grid stability risks. Some responses suggested that they had not identified any further risks outside of the scope of the consultation's proposals (3 mentions).

Other points included the need to ensure hot water systems were included in our smart mandate proposals (2 mentions), concern around Government over-regulating and having too wide of a definition of load control (1 mention), the lack of awareness of PAS 1878/79 amongst network operators presenting grid stability risks (1 mention). One response also outlined industry research on potential scenarios in which grid stability risks could arise, and the need to consider this as part of the next stage of the Government's policy development.

Government response:

The overall scope of the Government's proposals aims to ensure that the electricity system is secure, and all consumers can access all tariffs and DSR services, regardless of the device they have. We have not proposed specific interventions on certain entities from the outset, such as on EVs or home energy management systems, as this may unnecessarily increase costs or constrain market development. However, as noted in previous parts of this publication, the full details of what entities will be captured by our proposals will be subject to further consultation.

The Government is currently engaging with industry on the final scope of our proposals via the working groups. Industry representatives of affected parties will be invited into discussions on scope as part of preparation work for the next stage of future consultations. As part of this, we intend to discuss details of potential grid and cyber security risks in further detail with a range of parties prior to finalising our proposals in secondary legislation.

Analytical Annex

The analytical annex to the consultation attracted a range of insightful responses and new pieces of evidence. Government appreciates this and will use the new evidence to inform policy development. Further assessments of the impacts of intended Government policy will be published alongside future consultations. This chapter summarises the responses received for each question of the analytical annex.

AA01. Do you agree with the case for intervention and the market failures we have identified? Are there any points we have missed?

In the annex Government had identified market power, coordination failure and externalities as key market failures that were likely to hinder interoperability being achieved without intervention. Due to information asymmetry and misalignment of incentives consumers could be left exposed to the mis-selling of services, contractual lock-in or the mishandling of personal data. Government had further identified that firms may underinvest in cyber security or other measures to address grid stability due to externalities and imperfect information.

Out of 20 respondents, the majority (14) agreed with the Government analysis of market failures and the case for intervention. Six respondents did not express explicit support or disagreement. Some respondents emphasised that regulations must be balanced, and not hinder the current success of the market. A few respondents raised ‘equity’ as a further market failure and warned that there may be costs from the expansion of domestic DSR that, without intervention, could accrue to consumers who are unable to participate in, and thus benefit from, DSR.

AA02. 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?

Although there was consensus among respondents that the industrial DSR and ESA markets are more developed than the domestic ones, there were mixed views on the market’s current overall maturity. More specifically, some described the ESA market as fragmented, highlighting that some technologies (EV charging, battery storage) are being adopted at a faster rate than others. Some responses also pointed out that while a small number of time-of-use tariffs are available, the market is still underdeveloped. Others, however, were more confident in the current maturity of the market and listed a range of companies and providers currently active in DSR and ESA.

AA03.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.

There was consensus among respondents that the DSR and ESA markets will grow significantly to 2050. However, this was seen as dependent on Government interventions; adequate and clear incentives for industry and consumers; and the introduction of planned reforms. The planned reforms include the future homes standard, market wide half hourly settlement, and wider smart meter rollout.

AA04. Do you agree with the benefits of DSR we've identified and how do you see these changing over time?

In the annex Government had identified three main benefits of an increased level of DSR for the electricity system: (1) Reducing the overall cost of energy to all consumers, (2) enabling the power sector to decarbonise more cost effectively and (3) rewarding individual consumers for providing value to the energy system.

Out of 20 respondents, a significant majority (15) agreed with the Government analysis of benefits with five respondents not expressing explicit support or disagreement.

AA05. 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?

Respondents provided a range of helpful suggestions for the quantifications of cyber security benefits on a system level. These will inform Government analysis underpinning the design of future cyber security policy.

AA06. 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?

In the annex Government had identified additional costs to ESA manufacturers due to providing additional hardware/software to adhere to the Smart mandate and ESA requirements, the one-off costs of changing processes and systems (transition costs), additional technical, legal and managerial resource to read and understand the requirements (familiarisation), additional resource needed to provide after sale care (customer service), costs associated with governance arrangements and compliance costs.

Benefits specific to ESA manufacturers identified by Government include increased market size, reduced product development costs and increased international trade.

Out of 14 respondents, a majority (eight) agreed with Government analysis of benefits with 6 respondents not expressing explicit support or disagreement. Some respondents provided helpful detail on the cost items set out by Government. These will inform Government analysis underpinning the design of future ESA policy.

Answers to AA07 and AAO8 have been combined.

AA07. For firms in scope of the licence proposals, what type of costs and benefits might be incurred from these proposals?

And: AA08.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?

In the annex, Government had identified additional costs to load controllers in relation to the proposed extension of the NIS Regulations (if powers are granted to amend the regulations) and licensing proposals. These include costs associated with changing business practices to adhere to new requirements, the direct cost or fee associated with applying for the licence, monitoring and reporting costs, pass-through enforcement costs, learning, familiarisation and enforcement costs as well as governance costs.

Benefits specific to load controllers identified by Government include reduced risk of cyber-attacks and the associated reputational benefit, increased market size and reduced service development costs.

Out of eleven respondents, for AA07 and nine respondents for AA08 a significant majority (eight) did not express explicit support or disagreement with Government analysis. Two respondents agreed with the gov analysis on AA07 while one respondent disagreed. Some respondents expressed concern about the costs of complying with licence conditions and the disproportionate impact these could have on SMEs. Two respondents provided helpful insight on the costs related to the NIS extension proposal. These will inform Government analysis underpinning the design of future ESA policy.

AA09. 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?

All respondents agreed the system risk of a cyber-attack on load controllers at the moment is low since remotely controlled ESAs are currently not very widespread. As ESA deployment increases this risk grows significantly.

AA10. Are the costs and benefits identified for energy suppliers appropriate? Are there any we have missed, or not accurately specified?

In the annex Government had identified additional costs to energy suppliers due to one-off costs of changing processes (transition), ongoing costs to maintain and deliver solutions for time-of-use-tariff interoperability and the resource costs from supporting governance arrangements.

Benefits specific to energy suppliers include reduced costs of technical solutions and increased market size.

Out of five respondents a majority (three) of respondents did not express explicit support or disagreement with the gov analysis of costs and benefits with two respondents agreeing.

AA11. Are the costs and benefits identified for consumers appropriate? Are there any we have missed, or not accurately specified?

In the consultation annex Government had identified additional costs to energy suppliers due to pass through costs of meeting regulatory requirements and a reduction in consumer choice.

The main benefit set out by Government is a reduction of all consumer bills due to the reduction in overall system costs that a higher level of DSR will deliver. New functionality and increased consumer confidence enabled by several consultation proposals will allow individual consumers to achieve further bill reductions through utilising time-of-use tariffs. Proposals for ESAs to be interoperable with DSR service providers and time-of-use tariffs will ensure ESA consumers can take advantage of new offers, rather than being locked in. Consumers will further benefit from increased cyber security and consumer protection.

Out of 16 respondents an overwhelming majority (14) agreed with gov analysis of costs and benefits with two respondents not expressing explicit support or disagreement. Nonetheless three respondents questioned whether the bill savings achieved by using DSR services will outweigh the costs to individual consumers and flagged a need to carry out a more detailed cost-benefit- analysis.

AA12. 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?

In the annex Government had identified the following three distributional impacts: (1) The increased costs of products or services due to proposals could raise barriers to low-income consumers. (2) Product/ service complexity may require digital literacy and increased DSR update may increase inequalities between consumers who can and cannot access these products and services. (3) Consumers may incur barriers to using ESAs or DSR based on their location or the state of their premises.

More than a third of 17 respondents stated that Government action will be needed to enable domestic DSR services for low income and vulnerable households. Some respondents believed that providing equal access to low income and vulnerable consumers will be crucial in securing the overall consumer trust that a large-scale rollout of DSR services requires. Some respondents stressed that vulnerable consumers participating in DSR need to be protected from detriment. For instance, consumers with certain medical needs may consume electricity at peak times to power medical devices and should not be penalised for that.

Respondents identified additional barriers for low income and vulnerable consumers such as the lack of control over heating and EV charging devices for tenants, a lack of smart meters in homes, a relatively underdeveloped market for time-of-use tariffs, a lack of broadband connectivity and a lack of high-quality public information materials on domestic DSR.

One respondent raised the need that DSR services should not be sold to those customers for whom they are inappropriate and suggested the introduction of an affordability assessment DSR service provides should be mandated to conduct.

Government will use the insights provided by respondents to inform future appraisal of policy impacts.

Stakeholder engagement & next steps

Further consultations

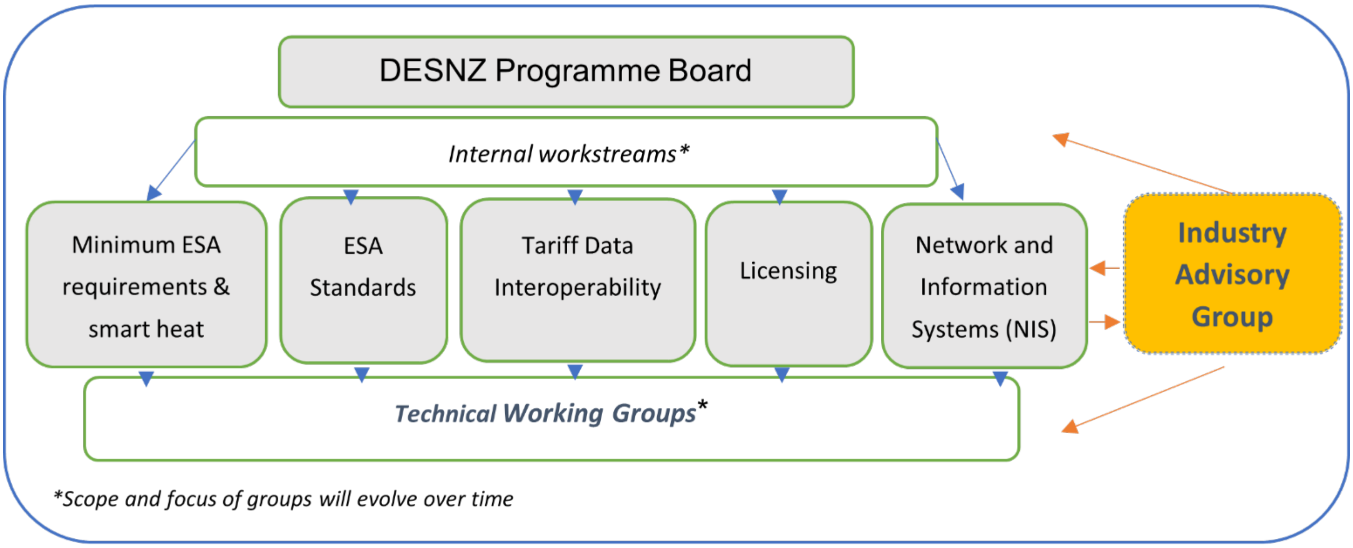
As noted throughout this publication, the benefits of our proposals to consumers, the industry and the wider electricity system could be substantial. However, further work is needed to finalise the details of the proposals to ensure these benefits fully materialise. Finalising the details of all proposals will involve further formal and informal consultation with industry and others on a wide range of specific topics.

Government will work with industry over the next year to 18 months to agree and finalise much of this detail. We will minimise burdens on stakeholders by consolidating the topics for formal consultation, either into a single document, or aligning publication timescales of multiple documents. The topics to be consulted on this year and early next year will include:

Topic to be consulted	*Details and timescales*
Smart heat mandate	Later in 2023, Government plans to consult on the details of how to implement our smart heat mandate decision including additional requirements on smart electric heating appliances, and the potential extension of the smart mandate to further electric heating appliances.
ESA Minimum requirements	Later in 2023, Government expects to set out more details on the minimum requirements expected of ESAs and proposed timescales for compliance.

Tariff data interoperability	Later in 2023, Government plans to set out the proposed technical and governance solution for interoperability of time-of-use tariff data.
Licensing regime for DSRSPs	Later in 2023, Government intends to consult on further details of our licencing regime. While we aim to have a licencing regime up and running by 2025, further consultation on the full remit of this regime will be iteratively developed, and the scope of the licencing regime will change as required in the future.
ESA Standards	Over the course of 2023, Government will work with industry via technical working groups as well as the National Cyber Security Centre and others to develop the detail of a future ESA standard based on PAS-1878. Given the breadth and depth of work needed to inform our approach, including consideration of potential common systems cyber security requirements, a consultation detailing further thinking on our proposed ESA standard will be published in early 2024 at the earliest.
Application of the Network and Information Systems Regulations	Timescales for future consultation on the detail of changes to the NIS Regulations will be dependent on primary legislation required to grant powers to Ministers to amend the NIS Regulations.

Stakeholder engagement


DESNZ Programme Board
Internal workstreams*
Minimum ESA requirements & smart heat
ESA Standards
Tariff Data Interoperability
Licensing
Network and Information Systems (NIS)
Industry Advisory Group
Technical Working Groups*
*Scope and focus of groups will evolve over time

Government will work with industry and others to inform the next stage of our policy development. We have started this process already by establishing an Industry Advisory Group made of up key associations and other organisations that will have a role or be impacted across all of the proposals detailed within this document. Separately to this, individual Technical Working Groups are being set up to feed into policy of individual proposals. For example, one group will focus on the work needed to develop an ESA standard that meets our confirmed outcomes. This group will guide the policy development needed for the consultation on the details of this standard. A further group will be set up to focus on cyber security policy proposals and issues. Further technical working groups will be set up as and when needed to inform further details of individual proposals. In some cases, informal consultation with relevant stakeholders will be done in absence of a formal established technical working group. Alongside this industry engagement informing our next stage of policy development, Government will also be incorporating learnings from our Interoperable Demand-Side Response programme[16] into our policy development.

Alongside this, the Government will also be engaging with international policy makers to best ensure international comparability on ESA standards, share best practice, and address common risks and challenges on flexibility, DSR, and energy smart appliances. The benefits of such engagement are already materialising, for example, the UK-US Energy Security and Affordability Partnership[17] sets out ways in which the UK and USA will work together to learn lessons on encouraging and preparing for greater use of energy smart appliances.

[16] https://www.gov.uk/government/collections/interoperable-demand-side-response-programme
[17] https://www.gov.uk/government/news/uk-and-us-announce-new-energy-partnership

Glossary

Term	Definition
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.
British Standards Institution (BSI)	The national standards body for the United Kingdom.
Cyber Assessment Framework (CAF)	The framework of that name established by NCSC to assist in carrying out cyber resilience assessments.
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 Provider	An organisation which provides a Demand-Side Response Service. Also DSR Service Provider or DSRSP.
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.
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 the Government's Net Zero Innovation Portfolio, that looks to support innovative solutions to enable large-scale widespread electricity system flexibility.
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 within the Government'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.
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.
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.
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.
Public Key Infrastructure	A system for managing cryptographic material that is used to secure and encrypt communications.
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	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.
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.

This publication 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 SSESconsultation@beis.gov.uk. Please tell us what format you need. It will help us if you say what assistive technology you use.