Department for Business, Energy & Industrial Strategy

Delivering a smart and secure electricity system

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

Response template

Closing date: 28th September 2022

July 2022

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

Invitation to respond to "Consultation on interoperability and cyber security of energy smart appliances and remote load control"

The consultation and supporting analytical annex is available at: 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.

The closing date for responses is September 28th 2022

Information provided in this response, including personal information, may be subject to publication or release to other parties or to disclosure in accordance with the access to information regimes. Please see the invitation to contribute views and evidence for further information.

If you want information, including personal data, that you provide to be treated as confidential, please explain to us below why you regard the information you have provided as confidential. If we receive a request for disclosure of the information, we shall take full account of your explanation, but we cannot give an assurance that confidentiality can be maintained in all circumstances. An automatic confidentiality disclaimer generated by your IT system will not, of itself, be regarded as binding on the department.

I want my response to be treated as confidential ☐

Comments: BEAMA is the UK trade association for manufacturers and providers of electrotechnical and electrical devices, systems and services. For more details of our views about the issues raised in this consultation and next steps, please see The Future of Smart Charging Report, co-written with Energy UK, which will be shared with BEIS upon publication.

Response form

Please complete the below pages with your information, and email it to us as a word document to SSESconsultation@beis.gov.uk

Or send it as a hardcopy by post to:
SSES team (NZEN)
Department for Business, Energy and Industrial Strategy
3rd Floor
1 Victoria Street
London
SW1H 0ET

Information about you and your response

What is your name? Jeremy Yapp

What is your email address? Jeremy.Yapp@beama.org.uk

(If appropriate) What is your organisation? BEAMA

Which of the following descriptions best describes you/your organisation?

- Private individual ☐
- Manufacturer ☐
- Distributor / Seller ☐
- DSR Service Provider ☐
- Chargepoint Operator ☐
- Energy supplier ☐
- Trade body ☒
- Consumer group ☐
- Energy network/system operator ☐
- Public sector body ☐
- Other ☐

Are you happy for your response to be published in full? Yes

Are you happy for you/your organisation to be named in a document summarising the responses received? Yes

As part of your response, have you included any other information separately from this consultation response template? If so, please provide a brief summary of what it is? No

Are you happy for us to contact you to keep you updated on the policy and consultation, including to notify you of stakeholder events and/or if we have follow-up questions on your consultation response? Yes

Consultation Questions

Questions detailed in consultation Chapter 1, "Introduction"

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

BEAMA's members generally support the proposed timescales seem broadly sensible; our reading of the consultation text is that the first set of requirements would not come into force before 2025, with the last set of requirements coming into force around 2029-2030.

However, we need to be certain that Government understands how "lead times" work in the context of global manufacturing supply chains and that it has learnt from the mistakes it made in the introduction of the Electric Vehicles (smart charge points) Regulations. Lead times for the sorts of device and system changes being proposed, including smart functionalities, cyber security and randomized delay capabilities, are likely to require significant design, component and integration modifications relating to hardware, firmware and software. It is likely that manufacturers will need at least 18-24 months (depending on the nature of the changes) – likely more. Note that this lead time does not refer to 2022 -> enforcement, or from the date of the Government releasing its "minded-to" position on this consultation. It refers to the time between the legislation being laid in and passed by both houses of Parliament, that is entering into law alongside the publication of official Guidance, and the time when the requirements take effects and are enforceable. Product development may not be able to begin in earnest until specific requirements are known.

Note that Industry cannot realistically begin to engage and invest in product development until these specific requirements are known, and it is at that point that a significant period – likely years, not months – would be required to implement any changes.

That said, Business is ready to invest. Capital is available and the motivation is strong. We are concerned that secure interoperability is difficult and time consuming (it has taken smart metering about a decade) and will be further complicated by the large number and diversity of stakeholders in the DSR environment.

There was a variety of views among the membership as to whether secure interoperability is best achieved with clear, detailed and unambiguous, preferably mandated, instruction on how to meet the secure interoperability requirements or whether "guidelines not rules" and a more open-source approach to interoperability and integration as well data was a better path. But either will take time.

We also agree with the general approach of phasing the policy introduction and agree that the progressive steps are sensible and allow business to adjust to the emerging policy landscape.

We warn against Government asking the manufacturing sector to "hurry up and wait", by which we mean facing challenging and expensive timelines for smart functionalities and products that are then delivered to the market ahead of need, before consumers are ready or before there is a diverse, vibrant energy market (whether based on energy services, flexibility, tariffs or whatever) ready to make use of the smart devices.

There should be a road-map of targets and deliverables for Government, National Grid, service providers, energy suppliers and the manufacturing supply chain (including a timetable for

regulatory requirements as well as for consumer uptake) that can inform a phased implementation approach. BEAMA, through its Energy Systems Strategy Forum, looks forward to more discussions with Government about how we can support this level of cooperation.

Questions detailed in consultation Chapter 2, "Cyber security proposals for protecting the energy system"

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.

We recognise the need for energy security and resilience of the energy system, and therefore that operators controlling significant capacity should be subject to appropriate cyber security standards.

Broadly we agree with this proposal. We recognise the risks inherent in allowing industry to control large quantities of electrical load and believe that some means of regulation is necessary to maintain appropriate levels of cyber-security, grid protection and interoperability.

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

Most members did not express a strong view on this question. We would just say that the Government should be very clear about what is means by "load" here, because a large number of connected devices may constitute a total load of >300MW, but only a fraction of that will be dispatchable or flexible, simply because most consumers are not active users of DSR.

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?

Total load controlled, total number of affected customers or properties with potential remote load control by an operator, and number of local electricity networks vulnerable to unplanned outage. Also: density of any ESAs connected to a single network (we understand that a 10% saturation of heat pumps on the network is enough to create a challenge for many substations that need flexibility services to address). For this consideration for local network constraints, we expect there to be some additional measure of DSO network approval for loads above a certain level.

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.

We have not identified any specific challenges in using the Cyber Assessment Framework to support the implementation of Network Information Security requirements for load controllers and there is a general agreement among members that all NIS requirements should be aligned.

However, on member noted that while the CAF is a useful framework for achieving a level of assurance, it has the potential to cause uncertainty and delay to manufacturers wishing to introduce new products. The lesson from smart metering is that, while we all agree that CPA (or a similar process) should be onerous and difficult, it could be made more efficient and no less effective. We would be happy to work with BEIS and NCSC to discuss in more detail how this process could be improved without compromising safety and security.

Questions detailed in consultation Chapter 3, "Energy smart appliances: Outcomes"

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

There is a lot of support in principle within Industry for the proposed outcomes for interoperability. Setting achievable minimum standards with open market protocols ensures maximum growth and innovation in the early stages. Early development of a standard interoperable interface should be done in the Cloud. The proprietary link from ESA to the Cloud should then interface with a standard set of functions which allow the ESA manufacturer to extract flexibility and present to the CEM. We invite Government to work with us to develop a standard set of library functions to which Cloud developers acting for the ESA manufacturer can "customise" for that manufacturer's needs.

However, even the limited proposed outcomes are currently not deliverable and it is not clear to us how it can be delivered. Supporting ToU tariffs from different energy suppliers and other minimum services from DSRSPs is beyond current technology of capability. We need a plan that makes sure the interoperability requirement does not translate into a race to the bottom, where interop is the primary aim and rich services with differentiated market offerings disappear because there is no incentive to provide them.

In summary: we understand the benefit of some level of interoperability for the consumer, but it needs to be balanced with retaining and incentivising innovation in the market.

Maintain tariff interoperability but removing DSR services from the requirement may be a solution worth considering.

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

The proposed outcomes seem appropriate, and we welcome the work of government and NCSC to complete the risk assessment of the future system of ESAs and DSR.

One possible addition to a future list (as the proportion of renewables on the Grid increases and generation becomes even more intermittent) is for DSR capability be classed as CNI, to reflect the growing importance of system flexibility.

We welcome an opportunity to work with Government and NCSC to manage the cost of compliance, given that it is consumers paying for it in the end. In particular, some of the wording used to describe physical tamper protection leaves open the prospect of frighteningly high costs (as has already been discussed and clarified, largely to our satisfaction, in relation to Schedule 1 of the EVSCP Regs). We also warn against over-specification: ESAs are not mandated smart meters and should not be subject to the same rules.

It is unclear at the moment where the smart functionality is going to sit (HEMS, for example, or the ESA) and too early to predict, so we should be allowing for both options to evolve. It is important to recognise that cyber security requirements are already built into a lot of communications protocols, for example Matter, and that doubling up becomes costly.

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

Broadly yes, recognising that in such a data-centric and complex system, data is important for the provision of future consumer benefits. Therefore, the minimisation of use of personal data must be balanced with consumers' ability to share this data with service providers if they choose, in exchange for benefits. We suggest a distinction between 'personal' data and 'industrial' data, where industrial data is used to enable ESA operators and manufacturers to ensure the safe and efficient operation of the device. In making such a distinction, industrial data should be restricted to technical diagnostic data and should be provided over a secure interface with the consent of the consumer.

Overall the data privacy principles are reasonable and in line with good practice, with the proviso that one of the "controls in place to protect against access by unauthorised entities" is the security of the domestic premises.

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

We agree that all risks identified in the consultation are relevant. However, grid stability risk assessments should take account of the inherent diversity offered by different ESAs. For example, a heat pump may be running almost constantly, albeit consuming variable amounts of power, whereas an EV charge point is likely to be used much less frequently. They pose different kinds and levels of risk.

We need to be very careful how we protect consumers from long delays (missing most of a half-hour tariff period due to a random delay is not a good customer experience) and how we communicate random delay functions to consumers. There are plenty of things that can go wrong here if not managed carefully.

We would like more clarity from DNOs (or other stakeholders) exactly how much flexibility and random-delay they need at the settlement edge, and we hope that most such delays will be seconds rather than minutes or hours.

Questions detailed in consultation Chapter 4, "Energy smart appliances: Technical frameworks"

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?

Yes. We agree that this is a key enabler of many innovative energy propositions and we encourage Government to expedite this policy. Although not widely available in the market, we note that smart meters also support block tariffs that may become more prevalent in the future. In addition, we propose that type-of-use tariffs, which have also begun to appear in the market, could be made openly available in a similar way.

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

The SEC could provide appropriate governance, but it is important to recognise that it has slow, unwieldy change processes that are slow to respond, and that it engages primarily with the energy retail sector. If the SEC were to be used as the basis for developing common data standards, government must ensure that it adequately caters for ESAs and ESA suppliers, not just energy retailers, and that the changes required can be delivered at low cost and at speed, so as to not slow down or stifle innovation in this fast-moving sector. To be fair, these changes to the SEC would be welcome in the context of its other work as well.

A lesson from smart metering is that means of testing interoperability are very important because it is very difficult to ensure interoperability through specifications alone. A significant testing and potentially a certification process may be necessary to provide assurance that interoperability can be achieved.

All that said, the Government needs to be very careful that it balances a robust and considered approach to standards development against the need for speed. The SEC as it currently operates is too slow, but there are few alternative models.

One option is a bespoke industry-led standards process that reflects the speed of development and change required by ESA and service suppliers, with (ideally) commercial standards' governance. But it may be more efficient to devise such a process and run it under the auspices of a more-inclusive SEC.

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

Existing regulations in this sector, such as the Electric Vehicles (Smart Charge Points) Regulations, are a good model for the requirements for ESAs.

This question can be split into two parts: 1) How are ToU tariffs made available to ESAs and 2) How is the integration of ToU tariffs to ESAs incentivised?

ToU tariffs could be made available in a standardised, interoperable format using established SEC data formats. This could be achieved by establishing a new DCC user role which permits read-only access to tariff information. This would require changes to the SEC to enable storage of the tariff data in the cloud and access to that data through a standardised API.

A simpler approach might be simply to use a consumer access device (CAD), perhaps incorporated within the EV charge point. This could ensure that the tariff data being acted upon is always accurate because it is being read from the meter, which is applying the price of electricity in the premises.

To allow innovation in the market, the DSRSP could be required by license to make tariff information available to the ESA; if the license does not stipulate how that is achieved, the market could then determine the most reliable and cost-effective means of achieving it.

We are generally in favour of commercial incentives being made available to ESA suppliers and service providers to motivate them to add ToU-related features, in the knowledge they will be able to offer value-added services in the future. That will encourage product and service innovation while still providing an underlying general interoperability.

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

Electricity network carbon intensity data should be made as openly available as possible, including any regional variations. Currently it is often only provided at the national level. This would help consumers wanting to use ESAs when electricity being supplied has the lowest levels of carbon intensity.

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.

In general, we favour outcome-based regulatory requirements, as these tend to support innovation best.

It is not obvious that a market for DSR will be viable. There is still much to be done, and much that can go wrong. A strong mandate for a specific technical standard would therefore be helpful, to reduce uncertainty about Government's requirements for ESAs and gives industry a clearer pathway for investment, boosting confidence; to reduce the time spent trying to make 'partially suitable' standards fit the requirements; to allow the specific and possibly unique GB requirements to be specified up front; and so that it does not preclude the use of existing standards where appropriate, for example for underlying communications transport (e.g. OpenADR.) However, Government needs to be clear about how these standards are to be implemented.

There was no unanimity amongst the membership as to whether a standard should be mandated or not. We suggest in the short term that the Government adopts a "guidelines not rules" approach, and that any mandate is on outcomes rather than methods.

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

Generally we acknowledge that PAS 1878 is the best starting point (no point going back now) for future ESA regulations, but we would like more time to discuss with Government in detail where the specification is less useful and to outline some suggested principles that we think are important when working for a better outcome (in terms of process and in terms of what we want an ESA to standard to enable/allow us to do).

PAS 1878 was developed in advance of any industry being active in working to the standards it sets out, so regulation based on some of elements of it may be appropriate, but it should not be relied upon entirely for the development of regulation.

Depending on the successful outcome of trials such as those proposed in the Interoperable DSR programme, PAS 1878 (with or without the use of the smart meter network) seems the

best option for achieving the minimum requirements for DSR while clearly setting out the boundary between regulated and non-regulated capabilities. By defining this boundary, it allows industry to offer non-regulated innovative solutions such as home energy management.

While it provides a good framework, but it does not cover the regulatory detail that would be needed to assure ESAs for connection.

One of the major architectural “decisions” taken in the PAS is that a DSRSP would be presented with flexibility options for every charge point and the ability to control them, via a mandatory interface (OpenADR). This could prevent CPOs from aggregating their devices to offer a service direct to the energy sector, unless they become a DSRSP themselves or move outside the architecture. It would also mean that the interface between the CEM and the DSRSP is likely to be generic, despite the device types having very different characteristics and use cases. Defining the interface in such a nascent market will stifle innovation as the industry is pushed to homogenise data flows from EVs, heat pumps, battery etc.

Commercially, it risks regulating CPOs down to a level of “device manager” and limit their ability to offer advanced services and incentives to customers. There needs to be an ongoing relationship with the charge point manufacturer and the customer, at a minimum to keep the device updated, online and functional. The PAS architecture risks reducing the manufacturers’ and CPOs’ commercial interests to do this, as the revenue opportunity would be diluted through a DSRSP.

CPOs have the potential to know much more about customers than can be transmitted through a standard interface and can categorize customers according to multiple criteria. Their business cases depend on their ability to offer targeted services based on this in ways that the PAS architecture puts at risk. This might be addressed by CPOs becoming DSRSPs themselves, but that would be an unintended consequence of these technical proposals.

We want to work through these issues with the rest of the sector and Government, for example to explore whether ESAs can be aggregated at the CEM layer and presented to the DSRSP as a single, larger entity (which could in turn bypass Interface A if the ESA manufacturer is providing an end-to-end solution) and to define the interfaces between on the grid management side of the DSRSP for flexibility requirements. These are not concrete proposals, merely examples of issues we want to work through with Government and other Industry stakeholders, indicative of how the lack of a standard interface at the CEM level is not the only significant barrier to unlocking flexibility value.

We also re-iterate that the PAS has not been tested in the field so we do not know how it will perform in an environment with highly distributed assets. The PAS is still at concept stage, not a mature, well tested specification, and much more work needs to be done before we consider regulation based on it.

In some cases, HEMS manufacturers will want to retain control of Interface A. Industry does not want to be making new protocols – it wants to be following (or leading) what is used internationally. We would oppose any divergence for EU standards unless there were very good reasons. BEAMA believes the UK can and should be a leader in this international market, not a niche.

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.

Government should focus its regulations on appliances that will deliver material amounts of flexibility. It should not attempt to regulate appliances that deliver small amounts of load, such as fridges, washing machines and clothes dryers. Initially it is more important to prove the viability of the technology and the market without attempting to incorporate appliances with minimal benefits. If the technology and market prove viable for large loads then regulation could be extended to smaller loads if required to meet net zero policy objectives.

With that in mind, the scope of “domestic-scale ESAs with the highest potential for flexibility” could be taken to include any permanently connected device delivering load that is (or can be) aggregated to deliver a meaningful grid load changes. This could apply to devices beyond those listed, such as water heaters, large refrigeration, and secondary controls, provided they are permanently connected loads able to be aggregated to deliver DSR services.

The behaviour, performance and usage ESAs vary, and standards should be written with this variability in mind. While the examples of ESAs referenced would seem to be relevant when considering those with the highest potential for flexibility, other devices should also be considered. The addition of direct-acting electric hot water cylinders and hot water heat pumps would add significant storage capacity with long-duration, year-round storage properties. This would also allow consumers the opportunity to save on what is often the greatest single component of an annual electricity bill.

These technologies have not been designed for this as-yet undefined role. So regulation for these technology categories must proceed carefully, with an eye to regulating for only those functionalities that are necessary to create value.

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.

It is very important that any regulations are aligned with global standards and that there is harmonisation of standards through global industry groups or associations. It is very

challenging to operate if significantly different standards emerge in different markets. There needs to be greater coordination between national governments, as well as regional bodies such as the European Commission, when it comes to the developments of standards in this sector.

There also needs to be effective cross-sector engagement, given the number of industries affected by the proposed regulations, from energy suppliers and ESA operators through to heat pump and EV charge point manufacturers. Broad sectoral engagement is key, with government and regulators ensuring that is it not only a narrow group of stakeholders or trade association representatives involved in decision-making.

Speed of implementation is important if we are to meet climate change objectives. A BSI-led approach has the advantage of being well-established and authoritative. However, the SEC modification process has also been used successfully to develop and maintain the SEC and could, with sufficient transitional governance provided by government, also be viable.

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

Storage is operating in a peak shaving or an export limiting mode requires a fast response capability that would clearly not be possible if a randomised delay were to be applied. The Government should note that EREC G100 stipulates <5 seconds currently and, for many manufacturers, peak shaving response is within the same sub-5 second time frame. This is perhaps less of a concern in residential applications but certainly would be concerning in small commercial applications, which may also come into scope.

From a grid stability perspective, it is worth considering alternatives to imposing a randomised delay that could deliver a negative consumer experience. For example, frequency response capabilities at the device level would reduce the reliance on direct signals from third-party platforms or providers and could respond more dynamically if there was an issue detected, rather than delivering a delay by default. Randomised delay may make sense for permanently connected and timed/automated devices but does not appear appropriate for ESAs that are used with an inherent degree of randomness or those that are typically not drawing power from the grid, for example domestic storage batteries. In addition, if randomisation is applied, it should only be required in relation to consumption from the grid connection point in the home. Devices using microgeneration or local energy storage for power should not need to be delayed.

If a randomised delay is to be introduced, it would make sense to replicate the requirements in the Electric Vehicle Smart Charge Point Regulations, rather than create a new set of randomised delay requirements for ESA providers, some of whom have already developed this functionality for EV charge points.

It is also worth considering the impact of longer delays on half hourly settlement energy tariffs – consumers will be disadvantaged by a randomised delay of 30 minutes (the maximum potential period outlined in existing regulations), meaning that they fail to benefit from cheaper energy tariff rates, for example.

Randomised delay is a well-established means of managing load discontinuities resulting from synchronised action of endpoints. It will be helpful in managing loads on both the communications networks and the electricity network. The technology exists and is low cost. However, where the delay is likely to be impractical or unacceptable to consumers, or where an instant response by the device is required (such as frequency based response (DC) DSR), randomised delay should not be required.

Has Government sufficiently explored whether a form of signalled delay can be introduced to cover mass reconnects or restarts and time based events, such as half hourly ToU changes?

We need to establish just how much of a delay is required. DNOs and energy suppliers need to be involved in this discussion. Engineers are saying they need to know what to do (how long the delay needs to be). Randomised delay could compromise (for example) the balancing mechanism, as it requires high accuracy on start/stop times. So, load controllers should be allowed to override the delay under certain stipulations.

Multiple DSRSPs operating in a local energy system and relying on implicit flex (such as responding to ToU tariffs) will need some form of constraint signal from the DNO, so devices can see the constraint and respond accordingly. Considerable network headroom may be needed to manage this. As stated above, network operators (etc.) should state how much grid stability, and therefore how much randomised delay, they will need. This should be considered at system level. The ESO and the DSOs/DNOs need to be thinking about how resilient the system is to herding behaviour and to lots of devices responding to the same signals. It is not just a problem for consumer appliances; it is a larger problem, and therefore the solution needs to be broader.

Randomised delay could also be applied at home level rather than at device level. For example, in Germany, with its smart meter roll out, rather than talking to each ESA there is a HEMS in the home that manages the load in the home. The signal is sent to the home and the internal protocol determines what is the best way to manage the energy within the home.

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?

It seems appropriate to replicate existing standards and not discriminate against EV charge points, which already have to meet minimum cyber security standards. Prior to implementation of enduring ESA standards, we recommend that minimum device-level cyber security requirements should be implemented for heat pumps, storage heaters, heat batteries and

batteries because of the potential for their combined load to pose a risk to grid stability in the event of a cyber attack.

However, we assume that BEIS is working with NCSC to establish the risks to grid stability as a result of cyber attack and we recommend that security requirements for ESAs should be considered on the basis of their risk level, not the appliance type. The requirements should apply to all connected ESAs capable of being remotely switched, above a threshold load to be determined based on the likely grid impact of mass switching.

DSRSPs are likely to rely on correct metering values for the successful management of load, regardless of the load type. Therefore any metering functions employed alongside ESAs should be protected from tampering to ensure they provide the correct values to the DSRSP.

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

We did not reach consensus on this question.

At device level, ETSI 303 645 is a detailed standard that arguably goes beyond minimum device-level cyber security requirements. It may be more appropriate to specify requirements that are based on ETSI 303 645, rather than fully mandate its implementation. ETSI 303 645 seems to be the de-facto standard across IoT and the UK Secure by Design standard also reflects much of its content. It is considered good practice, and at device level we are not aware of significant objections to ETSI requirements.

However, at system level ETSI 303 645 is a ‘basic hygiene’ scheme that may be inadequate for the protection of the GB electricity system when faced with the type of sophisticated cyber-attacks such as could be perpetrated by the more advanced hacker groups or state actors.

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?

If common systems are considered, there should be due consideration of the cost and time to implement and integrate them into suppliers’ existing systems. In addition, government should consider the risks of the inevitable centralisation of information that common systems would involve, including the complicated certification required for Public Key Infrastructure.

While trustless approaches to security are available (e.g. blockchain) it is not clear how interoperability can be achieved without a ‘single source of truth’ for the definition of the interoperable interface. Whether this is in the form of a centralised API broker or anomaly detection system which adjudicates on the integrity of messages, some form of reference standard must exist to ensure that the common interface that is at the root of interoperability is enforced. Otherwise interoperability is likely to erode over time or never be fully achieved.

There is a cost trade-off between a ‘central system’ vs ‘multiple systems’ architecture, where the total cost of multiple systems, each serving a small segment of the market, would intuitively seem to be greater, all else being equal than a single central system. (In terms of risk, the risk associated with the central system approach can perhaps be considered high impact / low probability whereas the multiple systems approach can be considered low impact / high probability i.e. their risk score as the product of impact x probability may be similar.) If a multiple systems approach, where many individual providers serve a small segment of the market, is a higher total cost due to having to operate multiple systems, then it will be important to understand whether the market can bear this cost. If the market is likely to be sufficiently large to bear the cost of multiple systems then industry will probably prefer this approach, given the greater scope for innovation and differentiation. However, this may be considered a high risk strategy because if the market does not develop in line with expectations, and the number of system providers remains low, then GB could be left with a small number of critical national infrastructure providers that may be subject to less scrutiny and oversight than could be implemented for a central system.

The most obvious application of a common system here is in anomaly detection. A catastrophic anomaly in a single large DSRSM system can impact the whole grid, almost instantly, so a system-wide anomaly detection & response solution is essential. Some of these are already present within the grid infrastructure, but they will need to be adapted for aggregated domestic loads. This concept may well need to be reflected in the DSRSM systems themselves, even to the extent that an ESA of the future may need to include a failsafe mechanism to mitigate clearly anomalous instructions

For a more detailed discussion of anomaly detection options, please see the response from SmartDCC (who are BEAMA members, and who have engaged in discussions with the membership on this and related topics over the past year or more).

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

If industry works to the regulatory timelines proposed in the consultation document, time will need to be provided for suppliers to integrate with any common systems. It is important that the speed of development in the sector is not inhibited, and that suppliers are given time to comply with any future regulations. We agree with the Government’s reasoning for discounting Option 2.

Option 1, extending the role of the DCC, could be feasible but various technical and regulatory issues would need to be overcome. Latency of messaging between DSRSPs and ESAs would be a particular concern.

Option 3 seems viable but could take a long time to establish as such is unlikely to be a suitable solution.

Option 4 carries a risk of lack of vendor choice, particularly if the business case for DSR is marginal or uncertain or if the scope of supply is unclear, leading to a small number of companies being willing to participate. Lack of vendor choice may lead to poor or inadequate service, and potentially de facto vendor lock-in. That said, is it likely to be both the fastest to implement and the most flexible.

Questions detailed in consultation Chapter 5 "Energy smart appliances: Delivery frameworks"

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

We recognise the need to ensure we have a smart and secure energy system. While accepting the overarching need for the governance of standards, testing, assurance and policy, again we strongly urge that this is delivered in line with the fact that ESAs are consumer devices, designed to deliver a service to consumers.

We need to focus on consumer experience. Interoperability is essential to this experience and will difficult to "add in" later. So if it is decided that interoperability is an essential requirement, it should be supported early in the deployment.

Transitional governance will be important for ensuring that the market adoption risks are managed in addition to providing other checks and balances on market development such as ensuring that the market develops in a way which is fair and accessible for everyone in society.

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

Assurance and testing requirements should reflect the fact that this is emerging technology in an emerging market. Requirements need to be clear and easy to understand, to support investment and innovation.

We suggest guidelines, not rules, and certainly in the early stages when innovation is so critical. Policy should maintain a commercial focus on assurance, building on the quality and assurance that is already available, rather than inventing something new. We particularly agree with the concept of risk-based assessment that is mentioned. An individual ESA is generally a "power" device, so even that brings a required level of assurance, although on its own it is relatively low risk. But collectively switched ESAs bring a much higher risk and their level of assurance in this context must be higher.

Device assurance, in particular, is well established and the level of testing has long been commensurate with the device usage. There should be little reason to change this approach for ESAs.

Self-certification is appropriate where the occasional occurrence of risks is tolerable and fallback plans are available. For example, in the case of DSR this may include occasional large-scale security breach, potentially including system blackouts, or the non-interoperability of some ESA brands. When deciding on the assurance approach, Government should consider whether this type of occasional risk occurrence is tolerable. This applies equally to ESAs and associated cloud systems.

Lessons should be learned from Smart Metering Device Assurance (SMDA) process, which was a good concept imperfectly implemented. If option 2 is mandated, consideration should be given to an automated test system which can speed up the process of achieving assurance. We agree that interoperability testing should include switching between DSRSPs to prove compliance and not just using emulators. BEAMA would be very happy to work with BEIS and others in industry to capture post-SMDA learnings and apply them to this 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.

There were a number of detailed discussions within the BEAMA group on this question. We respectfully direct Government to the responses of individual member companies to understand the breadth of views, and we look forward to working closely with Industry partners and with Government to determine the best approach to assurance.

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?

Yes, we support the introduction of product labelling, and think that the product packaging and also instructions should carry information on the benefits the product and its DSR capabilities offer. Digital labelling used alongside product images and descriptions could also support effective comparison between technologies, similar to that used for the efficiency statement of hot water systems and other energy rated products.

A central list of verified labelled products could also support verification and selection of DRS capable ESAs for consumers and specifiers alike.

It may help consumers if they could understand which products had been developed in accordance with GB security and interoperability requirements. However, any label and its meaning would need to be socialised through media campaigns so that consumers could understand the advantages of a labelled product and the disadvantages of a non-labelled product. The label on its own is probably not sufficient.

There is no single BEAMA consensus view on the value of a “DSR-ready” label; some members are of the opinion that this will be of value to consumers, while others think it may mislead consumers into thinking that the device is sufficient for DSR and that no other advances need to be made (such as for example a functioning flexibility market and an array of consumer-facing flexibility offerings from service providers).

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

If new costs are onerous or significant, they risk raising the price of ESAs to a level that would imperil the business case for flexible energy management. That must be avoided. Therefore, the current situation where testing and labelling costs are absorbed by ESA providers in the cost of the product and factored into its sale price is acceptable only if the new regulations do not introduce significant additional approval or product costs.

Where costs, for example relating to governance, apply to both the DSRSP and the ESA manufacturer and are difficult to apportion between them, they should be apportioned at the point closest to the end customer so that they can be bundled into the service price with least markup. This implies that the DSRSP should bear the costs of shared governance arrangements and pass these costs through to their ESO / DNO customers through their pricing.

Better understanding of the total available market will help to determine the appropriate cost recovery model. To help answer this question, it would be useful if Government could develop a micro-economic model or deployment scenarios which showed Government's intention for deployment, including timescales, for different appliance types. This will help business to assess the total available market size and therefore construct business cases for investment. Key to this assessment will be the extent to which Government intends to mandate DSR capability in new ESAs and from what date. Equally it will be important to understand whether DSR capability would be optional for new ESAs.

Questions detailed in consultation Chapter 6 "Smart Electric Heating"

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.

The smart mandate should also initially apply to electric stored hot water cylinders, both direct and indirect (if fitted with an immersion heater) and to domestic hot water heat pumps. Both technologies are well established, the former in the UK (see https://www.beama.org.uk/resourceLibrary/thermal-storage----a-vital-component-of-zero-carbon-homes.html) and the latter in Continental Europe and Asia. The DHW heat pump can be used in conjunction with smart electric storage heating or direct-acting heaters in small well-insulated properties enabling these properties to realize the benefits of the flexible energy market.

Initially, the only storage heaters that should be classed as ESA s are those classified by SAP as High heat retention storage heaters. This avoids the confusion created in the marketplace by brands that claim that their products are "storage heaters" or are an "ideal replacement for storage heaters", when in fact the thermal retention of these products is only a fraction of a conventional High heat retention heater. We recognize however that at some point in the future a product that has a little less storage capacity than a current HHR storage heater might still be of value for its flexibility benefits. We warn against over-regulating in this area; it may be worth waiting to see how such products emerge, and whether there is a market for smart versions without a need for regulation.

Other electric heating systems that can be controlled in a similarly smart way – such as infrared heating – could also be considered within the scope of the proposals, even if there is more limited DSR opportunity. We would be interested to explore with Government (and BRE, and others in Industry) the practicalities of a broader definition of smart heating, as anything that draws above a certain amount of power and has a quantified element of storage or flexibility potential.

Smart Heating Controllers currently play a significant role in controlling domestic heating of space and water. We consider these an essential component of the ESA family and they should be included in scope wherever they control a mandated appliance, taking on that appliance's obligation.

Given the slow pace of roll-out of heat pumps and other devices requiring a deep retrofit, Government should also consider a shorter term retrofit programme for ESAs that would facilitate a faster deployment and deliver flexibility services as they are needed in the next few years. Smart controllers could be fitted to existing electric heating devices (electric storage heaters and immersions) immediately, at relatively low cost (a few hundred pounds), delivering immediate grid-scale DSR through just a few thousand devices.

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?

As the market evolves and new technologies emerge, regulations should apply dynamically to ensure that there is a level playing field with fair competition.

Smart Controllers should be able to meet the standard voluntarily in the near term. Hot water tanks are particularity suited to flexibility, as they can generally take excess energy immediately and store it for when it is needed. Flexibility services, particularly to absorb excess demand, could be realised almost immediately by fitting an approved ESA to control a hot water tank (immersion).

(see our answer to Q28)

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

The additional costs to add the necessary functionality to convert any of the cited heating products should not significantly affect the price enough to offset the benefits which will accrue from participating in the flexibility market for any customer class.

While smart functionality is likely to add cost to any device, the most significant cost differential of smart electric heating vs. traditional or legacy gas or oil heating technologies is in the transition to electrification itself, rather than the smart connectivity as such.

There is significant debate on the “just transition” and how the transition to cleaner energy will impact low income and vulnerable consumers. It is made more acute as this group is most likely to be on the most expensive tariff – standard or pay-as-you-go – which will naturally exclude them from taking part in flexibility offerings.

If the Government is serious about protecting the fuel poor or other vulnerable consumers (not an assumption on which we express a confident view) then it should begin by taking urgent action to prevent pre-pay customers paying more for per unit of energy than the rates available to credit customers. Government should also look at specific, targeted flexibility initiatives that can directly benefit this group.

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

We agree with the definition as proposed but we note that there is no mention of a minimum threshold of storage or inertia, which implies that a heating product which has the technical communications functionality, but has no storage capability, could still be classified as an ESA, but offer no flexibility benefit. It may, therefore, be sensible to reward technologies based on the scale of their potential contribution, so a 1kWh panel heater and a 12kWh heat pump are not equally reimbursed.

We also advocate for consistency and longevity of regulations so that any greater specificity mandated in future does not end up being retrospectively applied. Overall we agree with this definition, when paired with more prescriptive definitions of what constitutes an ESA.

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

Heat pump and electric resistance heater manufacturers are seeking a more detailed specification of the requirements for meeting the smart mandate, and provided that is available in a timely manner an implementation date of 2025 is feasible.

But none of that is relevant if Government reveals the specific legislation and Guidance six months before it comes into force. Industry cannot realistically begin to engage and invest in product development until specific requirements are known, and it is at that point that a significant period – likely years, not months – would be required to implement any changes.

Government should focus on the importance of getting the best solutions for customers, and ones that work well, not ones that merely meet the regulations.

The focus should be on getting the right outcomes for the energy system and energy consumers, not on rushing the introduction of regulations that could compromise product quality, performance or impact on the energy system.

Another argument in favour of 2025 is that this aligns with the FHS, SAP11 and revised Part L of the building regulations and thus will allow for ESAs to be designed into future compliance portfolios for new and existing buildings. In this way the new system could incentivise these ranges and accelerate the uptake of technology installed, achieving a valuable market with competition at a tariff and technology level quickly.

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?

    Ban the removal of hot water tanks from properties and bring forward the date from which new-build homes must contain a hot water tank. Launch a funded advocacy campaign directed at consumers, installers, builders and investors to inform everyone about the value and importance of hot water tanks and other forms of thermal storage. Consumers should regard the hot water tank as a vital technology for domestic energy efficiency, flexibility, cost-saving and decarbonization – alongside the heat pump, battery, EV or rooftop solar panel.

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

    Yes. Government should consider introducing a smart mandate for domestic-scale battery systems

Questions detailed in consultation Chapter 7 "Regulation of organisations"

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?

Some members acknowledged that companies already licenced to provide DSR services (through larger industrial loads) could have reduced licensing requirements or even possibly exemptions, subject to certain criteria, but currently this seems insufficiently clear and transparent. There was a recognition that measures may need to have a different focus, perhaps less concerned with interoperability, but the similar risks to grid protection and perhaps also cyber security and data privacy for the consumer would seem to apply.

A more general response is that licensing should apply for larger scale non-domestic customers. One of the purposes of licensing is to protect the electricity system from risks that could result in wide scale loss of power. Also, exempting large-scale non-doms creates potential regulatory disparities in the market.

It is not immediately clear to us how existing mechanisms or regulations for excluded sectors are sufficient – for example the potential for DSR services on residential focused on-street charging infrastructure.

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?

Any licensing framework should not limit or inhibit the speed and flexibility of innovation. It should be primarily service-related. Consumers are likely to want a single DSRSP across a range of products, so the licence should be constructed accordingly; multiple levels of licence may create too much complexity.

After some internal discussion, we refer you to the Landis+Gyr response for a detailed discussion of identified rationales for a licensing framework.

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

We broadly agree with the design principles. Any licensing framework should be fair and should recognise the impact of cost and time on this nascent and fast-moving sector.

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

While some universal basic standards or licenses may be required for all participants, it may be necessary to place more stringent requirements on the largest providers who may be managing higher levels of risk. Proportionality should be supported by a clear and simple licencing scale, probably based on scale (number of devices / switching capacity), geography (location of ESAs) and diversity (a more diverse set of ESAs is arguably less risk prone).

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

Existing consumer protection law is likely to be sufficient, at least in the short term. Government should allow time for the market to evolve and for nascent services such as DSR to mature before considering any further levels of consumer protection.

While not a risk for consumers directly, one member highlighted the risk of so-called ‘hostage-taking’ in the DSR market whereby DSRSPs intentionally increase loads in such a way as to create the need for DSR services to mitigate those loads. This ‘gaming’ of the system is unethical and ultimately damages the reputation of DSR and the efficiency of the electricity system as a whole. Protection from this type of behaviour may need to be included in legislation if not already covered.

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

Existing GDPR protections are sufficient, except for an identified gap in cyber security requirements (for example encryption) to protect data at rest and data in transit.

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

Licensing requirements could be appropriate to manage cyber security risks, alongside the other measures outlined in the proposals. They would need to cover the key cybersecurity requirements for DSRSMs operating below NIS level – technical measures, independent review, independent testing, etc. Proof or demonstration that appropriate measures are in place could simply be a pre-condition of a successful licence application. Measures could also be applied differently depending on scale, through the type of licence offered.

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?

We support this proposal. The market should remain dynamic and competitive.

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?

Yes. Conditions should include: systems sufficiently robust to manage grid stability concerns, financial sustainability and customer protection, the technical conditions discussed throughout this consultation, security of operations and personnel, cyber-security assurance standards.

Again, the approach should be scalable, depending on risk: DSRSPs managing larger amounts of load should be subject to stricter requirements.

Questions detailed in consultation Chapter 8 "Next steps"

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?

It is important that the proposals cover all potential load controllers. Regulations should place on the 'primary' load controller (probably the ESA supplier) a requirement for a 'failsafe' to shut down any third-party access in the event of any grid stability concerns.

Electric vehicles, in addition to EV charge points, should be covered by these regulations or other measures appropriate to EVs. There would seem to be limited value implementing cyber-security measures for the charge point when system-impacting load control, and accompanying grid instability, can be achieved equally through the vehicle API which is not subject to the same security controls.

Analytical Annex Questions

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

   Click here to enter text.

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

   Click here to enter text.

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

   Click here to enter text.

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

   Click here to enter text.

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

   Click here to enter text.

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

   Click here to enter text.

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

   Click here to enter text.

8. For larger load controllers, in scope of the NIS extension proposal, are the costs and benefits identified appropriate? Are there any we have missed, or not accurately specified? For example, what is your current level of cyber security spending, and what

~~additional spending would you anticipate in using the CAF to comply with NIS? Are you able to separate costs into categories, such as familiarisation, compliance reporting and incident reporting, or any others?~~

~~Click here to enter text.~~

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

~~Click here to enter text.~~

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

~~Click here to enter text.~~

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

~~Click here to enter text.~~

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

Alongside these proposals, there is a clear need to accelerate the changes being proposed in the Review of Electricity Market Arrangements (REMA) in order to remove the historic link between wholesale gas prices and electricity prices.

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

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