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: Click here to enter text.

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? Dr Ola Michalec

What is your email address? Ola.michalec@bristol.ac.uk

(If appropriate) What is your organisation? University of Bristol

Which of the following descriptions best describes you/your organisation? **I am a researcher of regulations surrounding cyber security of critical infrastructures and digitalisation of the energy sector. I am also a Policy Engagement Associate for the UK National Research Centre on Privacy, Harm Reduction and Adversarial Influence Online**

- 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? Click here to enter text.

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, I would love to engage in the development of these proposals through follow up meetings. I am also happy to share further information about my research, including preliminary results that are in peer-review**.

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?

As we're in the early stage of adoption of ESA technologies, we have a chance to mandate appropriate security, interoperability and privacy requirement from the earliest stage, i.e. following 'by design' principles and baseline minimum standards. Prioritising these actions *before* these technologies penetrate the market is crucial, as these appliances risk locking consumer in unsustainable practices for decades to come. Otherwise the adoption of ESA will face similar issues to consumer IoT: prevalence of cheap, poorly produced products that are made to break, that can be easily compromised and lose consumer trust through data leaks publicised in the media. I recommend connecting with the recent work from the UCL team (Brass, Tanczer and Carr) who analysed the issues from the evolution of IoT security standardisation – there are many parallels with ESA (e.g. https://digital-library.theiet.org/content/conferences/10.1049/cp.2018.0024)

In order to set implementation timings that meet the twin goals of digital security and sustainability, I recommend analysing your adoption curve foresight against the CCC's recommendations on rapid decarbonisation (https://www.theccc.org.uk/wp-content/uploads/2020/12/The-Sixth-Carbon-Budget-The-UKs-path-to-Net-Zero.pdf)

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.

   Yes, and it is worth noting that according to your suggested framework (mid 2020s), NIS Regulations will enter its second iteration (NIS 2) – at least in the EU (https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-review-of-the-nis-directive). The key feature of NIS in the EU will be the extension of the scope from 'the operators of essential services' to 'most medium sized businesses'.

   While the UK response to the EU legislation is not finalised, we can expect a similar scope change in order to help with coordination of international markets (ESA manufacturers are often international companies)

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.

N/A

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?

   If the UK govt was to follow the EU suggestions on scope expansion of NIS, I recommend that sectoral Competent Authorities reach an agreement with regards to thresholds and metrics.

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.

   Broadly, yes. However, we need to execute care when proposing what CAF is for. Some sectoral Competent Authorities treat it as a checklist that helps with **compliance**, whereas others (e.g. Energy CA) encourages using CAF as a **gap analysis tool** and de-prioritises the idea of 'reaching green' in the assessment. The purpose of CAF needs to be clearly communicated to the Operators so that they can focus on the right actions and avoid conflicts between the executives and technical workers. CAF can serve either of those purposes but not both at the same time.

   The important thing to note about the energy sector, especially if NIS scope was to be extended is the sheer diversity in cyber security capabilities and expertise. Through our research with NIS stakeholders, we found that for organisations with little to no expertise, a set of baseline expectations (twinned with asset discovery and asset management) to comply against is a useful tool to begin the cyber security journey, however for experienced organisations, compliance approach reduces their ambition and leads to 'thoughtless' cyber security assessments.

   We also found that encouraging semi-formal working groups and information exchanges worked well for collective capability building. We spoke to organisations across water and energy sector who formed such groups in order to benchmark their CAF responses, find commonly occurring gaps in practice and share information about levels of investments. These initiatives helped NIS to become a collective action rather than individual compliance exercise.

   You can find the details of these findings:
   http://www.bristol.ac.uk/media-library/sites/policybristol/briefings-and-reports-pdfs/2021/PolicyBristol_Briefing110_Michalec_regulating_digitisation_infrastructure.pdf - briefing
   https://onlinelibrary.wiley.com/doi/10.1111/rego.12423 - full paper

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

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

   N/A

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

   I agree that the systemic understanding of ESA cyber security is in its early days and support commissioning of further work, such as NCSC research referenced in the document.

   Based on my research with the stakeholders working on energy system digitalisation and cyber security risks, I suggest the following 'conversation topics' that need further understanding within ESA organisations.

   - How can we better monitor and report on the security of our systems over time?
   - Do you know what systems you have, how they are connected, what information they hold and who uses and controls them?
   - How do we establish thresholds for anomalous events in regular monitoring?
   - Where are our claims about the levels of risk come from?
   - How can I better understand what X vulnerability/threat actor means to our organisation?
   - How can we learn from well-publicised past cyber attacks?
   - Which lessons aren't transferrable to our sector/organisation?
   - What is the budget for maintenance of this security measure for X years?
   - What is the budget for upgrading this legacy system? How does it compare to the cost of dealing with a cyber incident?
   - **Dependency mapping:** What suppliers, assets and people are we the most dependent on? What can we afford to go down and what can't we afford to go down?
   - **Cascading risks mapping:** What happens to your organisation and customers if a particular computer system goes down? What are the consequences in terms of finances, recovery time, safety, equipment damage, disruption of services? How long can we continue business as usual in the event of a system/data outage? How much data loss can we suffer before business-as-usual processes are interrupted?
   - **Incident response planning**: What would a proportionate response to the worst-case scenario look like? If a major cyber incident happens, how do we share information in order to stop it happening repeatedly, share the lessons and learn together?

   You can access the report here https://petras-iot.org/wp-content/uploads/2022/03/How-to-talk-about-cybersecurity-of-emerging-technologies.pdf. The academic paper is currently in review

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

   I find that the understanding of privacy is too narrow in the document and it should extend to the following online harms typical to the energy sector
   - Surveillance of tenants based on smart home data
   - Abusing by-stander privacy (e.g. a tenant who shares a house with an owner of smart energy products but is not a named bill payer)
   - Unwanted personalisation of services based on inference of sensitive information
   - Third parties profiteering based on personal data (loyalty schemes, insurance)
   - Discrimination based on unfair tariffs and customer segmentation

Source:

Protecting data privacy is key to a smart energy future

https://ora.ox.ac.uk › objects › files

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

   N/A

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?
    N/A

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

    N/A

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

    N/A

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.

N/A

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 document rightly outlines that both approaches have their benefits and risks. In addition I would like to add the following considerations based on my research (publication in review – happy to share manuscript on request)

    Outcome based regulations
    * are currently favoured by the UK actors (see the shift of the NCSC cyber essentials to be principle based or CAF positioned as an outcome-based document)
    * enable agile innovation, interpreted flexibly by particular organisations
    * hinder benchmarking and comparisons across organisations
    * are more suitable for organisations that have an already developed understanding of cyber security so they can interpret the principles accordingly
    * without the above, the flexibility and subjectivity of outcome-based regs can risk leaving the sector in the position of regulatory capture
    * are likely to be set in collaboration with practitioners from management, business continuity and other departments

    Mandated standards
    * are more conducive to building a shared understanding of security across the sector and benchmarking
    * might slow down iterative development and rapid innovation
    * are more suitable to organisations that are early in their security journey and need to cover the basics
    * are likely to be developed by a narrower set of technical experts

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

    N/A

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.

    N/A

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.

    I would like to stress that regardless of the option chosen, the deliver approach needs to consider the stakeholders present in the room in order to identify and advocate against online harms to the citizens. In our research with 30 digitalisation stakeholders in the UK, we found that organisations that represent the interests of citizens and underrepresented in comparison with industry actors like ESA manufacturers. In further policy engagements, these organisations should be prioritised and equipped with capabilities to assess against any inequalities harms resulting from ESA. I am happy to provide a manuscript of the paper (in review) for further information

    In addition, I would like to emphasise the role ok UK Research Centres in identifying and mitigating against online harms caused by ESA. For example EPSRC funded PETRAS (https://petras-iot.org/) has a significant strand of research on energy while REPHRAIN (also EPSRC funded https://www.rephrain.ac.uk/) works on a systematic review and metrics for citizen oriented harms across the sectors. In one of my roles, I work as Policy Engagement Associate at REPHRAIN and my role is to communicate findings of over 100 researchers to relevant policy makers – I am happy to make relevant connections and start conversations. We are also launching a Strategic Funding Call where we're very happy to prioritise funding applications for proposals deemed as a priority by the policy makers – please contact me for further information.

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.

    N/A

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?

    Yes, they could be implemented as soon as possible to enable timely and safe decarbonisation of the grid.

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

    N/A

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?

N/A

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

N/A

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?

N/A

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.

N/A

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.

N/A

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?

N/A

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

N/A

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.

N/A

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?

    N/A

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?

    N/A

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.

    N/A

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

    N/A

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?

    N/A

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

    N/A

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?

    N/A

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?

N/A

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

N/A

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

N/A

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

N/A

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?

N/A

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.

N/A

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?

N/A

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?

N/A

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?

    N/A

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?

   N/A

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?

   N/A

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.

   N/A

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

   N/A

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?

   Energy sector operators should be encouraged to report ongoing threats in a confidential (rather than only executed breaches and incidents) so the CAs get a better idea of the scale of the issue.

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?

   N/A

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

   N/A

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?

   N/A

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?

   N/A

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

    N/A

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

    N/A

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?

    N/A

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.