

This document is classified as **White** in accordance with the Panel Information Policy. Information can be shared with the public, and any members may publish the information, subject to copyright.

Paper Reference:	SECP_107_1208_06
Action:	For Discussion

BEIS Consultation: Delivering a smart and secure electricity system. The interoperability and cyber security of energy smart appliances and remote load control

1. Purpose

This paper provides an overview of the BEIS consultation on interoperability and cyber security of energy smart appliances and remote load control, and its potential impacts to the SEC. A copy of the consultation may be found using the following link [BEIS consultation delivering a smart and secure electricity system](#). The Consultation closes on 28 September 2022.

The Panel is requested to note the content of the paper and provide feedback on the initial draft response, included as Annex 1 to this paper.

2. Summary Consultation Proposals

2.1 Overview

The consultation focuses on options for the implementation of powers set out in the Energy Security Bill through secondary legislation, subject to Parliamentary approval.

The Energy Security Bill introduces proposals to regulate and set minimum standards for certain Energy Smart Appliances, (ESA) including minimum technical requirements for cyber security, interoperability, data privacy and grid stability. The bill also mandates that electric heating appliances must have smart functionality, prohibiting the sale on non-smart appliances in G.B. This power also extends to private Electric Vehicle (EV) charge points.

The Energy Security Bill also includes proposals to regulate activities related to load control, ensuring that parties remotely controlling load operate in a way which is beneficial for consumers and the grid, for example meeting requirements for consumer protections and cyber security. Activities in relation to the provision of load control will be licensable.

There will be a phased approach to the delivery of the proposals, as set out in Table 1 below;

Phase	Proposal
Short Term (by the Mid-2020s)	- To require energy suppliers to make time of use tariff data openly available in a common format, accessible over the internet. - To require domestic scale ERAs, including heat pumps, storage heaters, heat batteries and batteries, to meet minimum cyber security and grid stability requirements, similar to those recently established for private electric vehicle (EV) charge points.
Mid Term (Mid– 2020s)	- To require heating appliances with the greatest flexibility potential, namely heat pumps, storage heaters, and heat batteries, to have “smart” functionality. - To establish a proportionate and flexible licensing framework for organisations providing DSR to domestic and small non-domestic consumers. - To require large load controllers to comply with the provisions of the Network and Information Systems (NIS) regulations, and to be assured by the National Cyber Security Centre (NCSC) Cyber Assessment Framework.
Long-Term (Mid-late 2020s)	To require larger domestic scale energy smart appliances, such as EV charge points, batteries, and heat pumps, to be fully interoperable with Demand Side Response (DSR) service providers, and to meet further requirements for cyber security, grid stability and data privacy.

Table 1 – High level phased approach to implement proposals

2.2 Proposals and impacts to Energy Smart Appliances (ESA)

The term Energy Smart Appliances within the consultation refers to heat pumps, heat batteries, storage heaters, batteries, EV charge points and other white goods and heating appliances.

Table 2 below, shows the impact of the proposals in relation to the different types of ESA

Type of ESA	Proposal
Heat pumps, Heat batteries, storage heaters	- To require new appliances to have “smart” functionality - To meet minimum cyber security and grid stability requirements, similar to those already in place for EV charge points - To be interoperable with DSR service providers, and to meet further requirements for cyber security, grid stability and data privacy
Batteries	To meet minimum Cyber security and grid stability requirements, similar to those already in place for EV Charge points

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

Table 2 – Impact of Proposal by ESA

Delivering ESA device interoperability, as envisaged by the policy intent, will require a minimum set of functionality. ESA will be interoperable so that ESA devices can receive and respond to Time of Use information from different energy suppliers and provide Demand Side Response services in a secure environment. Figure 1 below illustrates how this may work in practice.

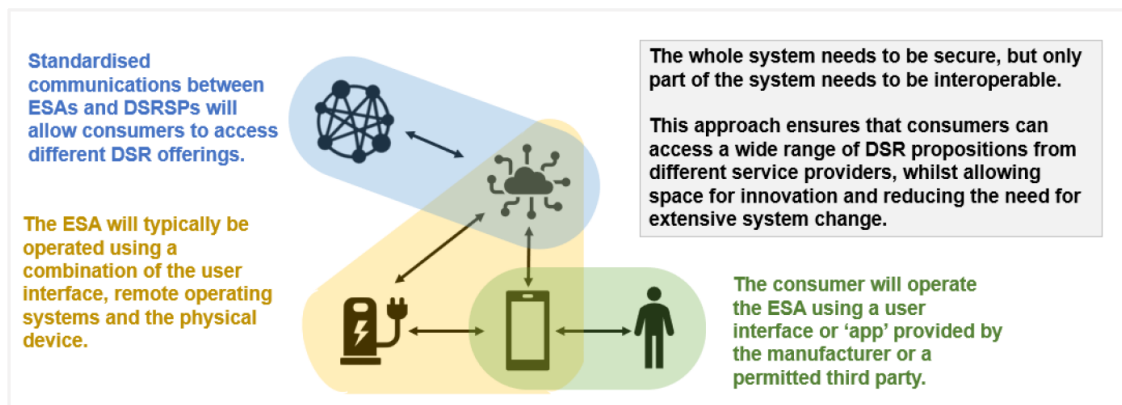


Figure 1: DSR Service Provider Interoperability – illustrative implementation example

2.3 Summary Consultation Proposals

- ESA must have smart¹ functionality
- ESA must be able to receive and respond to Time of Use (ToU) tariff information
- ESA must be able to provide Demand Side Response
- Implementation of minimum standards for cyber security, grid stability and data privacy for ESA and Load Controllers (the organisations who will be able to control ESA, in effect

¹ Smart functionality is defined as: *in relation to a device, the ability of the device to respond in real time to remote communication signals, using digital technologies, to deliver a service.*

potentially increasing or decreasing electricity demand) ultimately based on European Telecom Standards Institute (ETSI) EN 303 645

- Implementation of licence requirements for load controllers (controlling more than 300MW of load) and cyber security via NCSC NIS arrangements
- Adoption of interoperable Demand Side Response Standards based on Publicly Available Standard (PAS) 1878

3. Areas within Consultation with Potential SEC Impacts

The following are specific themes, taken from the consultation, that SECAS has identified as potentially having an impact or developmental interest for the SEC.

3.1 ESA Data: Time of Use Data

ESA will receive and respond to Time of Use (ToU) tariff data. The consultation notes that there is a lack of a reliable and consistent approach for consumers and manufacturers to access ToU tariff data.

The consultation proposes to require energy suppliers to make ToU tariff data interoperable, by being openly available in a common format. The consultation proposes to place a requirement on energy suppliers via an amendment to supplier licence conditions.

In addition, a technical solution is required to enable access to ToU data in a common format. Such a solution may be developed and maintained by industry codes to manage and govern the process.

The consultation proposes that the SEC could provide appropriate governance to develop these arrangements, building on the current role the SEC plays in standardising smart metering data.

3.2 Energy Smart Appliance Interoperability Standards & Minimum Standards for Cyber Security

ESA standards are proposed to establish how ESA must operate and interact with DSR providers. Government is seeking views via the consultation on the most suitable approach. The government proposes two options to promote the adoption of ESA standards;

- Option 1 – outcome based regulatory requirements and “presumptions of conformity” through approved standards”

This option would allow a dominant standard to emerge, without preventing new approaches and innovation, through approval of open standards overseen by governance arrangements across industry. However, this option could increase complexity, introduce interoperability challenges, and increase cost for DSR Service Providers and end consumers.

- Option 2 – Mandated Standards; through legislation or through industry codes.

This option provides certainty for ESA and DSR service providers and would be simpler to enforce, but may, overtime, reduce innovation.

Either option provides an opportunity for development of the SEC to oversee and raise awareness of the requirement to adhere to “*the standard*”.

The consultation proposes that a standard based on PAS 1878 is used in future regulation of ESA. The consultation notes that PAS 1878 will likely require amendments before this could be deployed at scale, in particular updates, required for Virtual Lead Parties participating in settlement.

The consultation notes further work with the NCSC will be undertaken to develop detailed requirements and potential amendments for PAS 1878.

The consultation recognises ESA can have a detrimental impact to the grid through synchronised changes in load and raises questions as to how best to manage these risks. Options include, randomised delay of up to ten minutes, which is already mandated for EV charge points, and could be extended to other ESA, if broader standard based mitigations are required.

The consultation also discusses issues of cyber security risks for ESA, and what appropriate standards should be applied, for example adoption of an existing international standard (ETSI 303 645) would mitigate risks for connected devices.

3.3 Common Systems – Communication Networks

Whilst government is not expecting to prescribe an ESA communication platform, there is an overriding need for interoperability and to ensure communications are secure. Dependent on the security requirements needed, an option would be to extend the role of the DCC and thereby the DCC licence to provide a common and secure platform for communications. This approach could use the existing procurement role of the DCC to leverage synergy benefits. Alternative approaches considered:

- Create a new licensed common service provider
- Establish a new body to procure systems
- Establish a list of “approved” service providers.

If the DCC is determined as a preferred model, there is a strong possibility of further changes to the SEC and related governance regimes to reflect the new service and changes to DCC Licence.

The consultation notes that a detailed risk assessment is to be completed before a decision on a common delivery approach for communications.

The consultation notes that BEIS is carrying out work with NCSC to develop a security architecture that will establish Public Key Infrastructure (PKI) within an interoperable DSR system for ESA. New service providers may be required to provide certificates. Anomaly Detection is also referenced as potential mitigation to prevent adverse impacts to grid stability. PKI and Anomaly detection are techniques used within the SEC to manage risks to smart metering.

3.4 Delivery Framework

The consultation contains proposals for an overarching delivery framework, to deliver the policy proposals. Broadly 3 phases of delivery are expected.

- ‘Development’ of governance, plans, designs & security arrangements

- 'Transition' to an interoperable ESA standard, assurance regimes, common systems
- 'Delivery' where long-term arrangements are established for sale of compliant ESA

The government intends to establish governance for the development phase and initially manage industry groups, with a view to handing over responsibilities under transition arrangements.

The consultation considers two options for the transition phase:

Option 1 - Establish a new, not-for-profit, delivery body. The systems, processes, governance, cost recovery mechanisms would need to be set up, similar to various energy industry bodies (e.g. SECCo or RECCo) or Open Banking Implementation Entity.

Option 2 - Build on SEC governance arrangements. Extend the existing arrangements to enable SECCo to manage ESA-specific codes.

Option 2 would increase the scope of the SEC, although no preference is stated in the consultation. This presents an opportunity for SECCo to increase its scope and work across the broader ESA environment.

4. Next Steps

Following discussion and feedback from the Panel, SECAS will further develop the consultation response and return to Panel in September seeking formal approval to submit the response.

The consultation is also being discussed at the August 2022 TABASC and SSC meetings, and feedback will be incorporated into the final response.

5. Recommendation

The Panel is requested to;

- **NOTE** the contents of this paper;
- **DISCUSS**, and provide any additional **FEEDBACK** for inclusion in the Panel response by 30 August 2022.

Tim Newton

SECAS Team

5 August 2022

Annex 1 Draft Response

Peter Davies, SEC Panel Chair
Smart Energy Code Company Limited
8 Fenchurch Place
London, EC3M 4AJ

By email
SSEconsultations@beis.gov.uk

[28] September 2022

BEIS consultation: Delivering a smart and secure electricity system; consultation on interoperability, cyber security of energy smart appliances and remote load control

Dear Sir / Madam

The SEC Panel is pleased to provide its response to the recent consultation on interoperability, cyber security of Energy Smart Appliances and remote load control. The SEC Panel is supportive of the approaches outlined, and will be pleased to work closely with BEIS, to exchange views and share experience, to facilitate the development of the ESA and Demand Side Response (DSR) market.

Not all of the questions in the consultation relate to activities or actions that may be undertaken by SEC Governance. This response therefore sets out Panel views against the themes and areas within the consultation, that have been identified with the greatest potential for SEC to assist with future development and implementation.

The rollout of Smart metering, and the governance framework of the SEC, was originally envisaged as an enabler for wider “smart” activities, towards the overall net zero goal. The Panel is therefore keen to build on appropriate smart metering technical and governance capability, to assist BEIS in its broader aims.

1. Provision of Time of Use Data in a Common Format

The Panel, along with its Sub Committees, supported by SECAS, has extensive experience of managing devices to minimum specification, security and privacy standards. For example, parallel may be drawn with the proposals to publish Time of Use (ToU) tariff data in a common format, to the Central Product List (CPL) within the SEC. Devices must meet the CPL requirements set out in the SEC (Appendix Z) to be added to the CPL. Devices that do not meet the requirements of the CPL, cannot be added by the Data Communications Company (DCC) to the Smart Metering Inventory and cannot be communicated with.

SECAS manages entries to the CPL on behalf of the SEC Panel. The CPL is published on the SECAS website in a standard format for industry to view, in both technical and plain English versions. A similar approach could be developed for energy supplier ToU data and made available for ESA manufacturers, overseen through SEC governance, so that any future changes are appropriately assured, documented, and managed for industry.

2. Energy Smart Appliance Interoperability Standards & Minimum Standards for Cyber Security

The proposal that ESA and DSR service providers meet certain cyber security standards is sensible given the potential risk to Critical National Infrastructure.

The SEC Panel supported by the Security Sub Committee and SECAS, oversees security assessments of SEC Parties, to ensure that the security requirements within the SEC are being observed. Comparison can therefore be made with the proposals for cyber security standards for ESA. Privacy obligations within the SEC are also overseen by SECAS on behalf of SEC Panel, to ensure Parties adhere to the requirements appropriate to their role.

The consultation notes further work is needed to assess the Publicly Available Standard (PAS) 1878 for ESA and the European Telecom Standards Institute (ETSI) 303 645 standard for cyber security. Initial discussions have been held by the SEC Panel Technical and Business Architecture and Security Sub Committees, (TABASC and SSC respectively) to consider potential technical and security impacts for smart metering.

At its August meeting, the TABASC raised concerns over timescales for implementation given the current challenges facing the smart metering architecture. Trying to incorporate more functionality may prove challenging for the DCC, at a time when the basic smart metering delivery should be paramount. The TABASC also consider the DCC would be a good fit for many of the proposed measures, albeit accept that there may be alternatives, but it is not clear who or when. The TABASC also felt that there isn't an understanding of the landscape when it comes to the future of ESA or the way DSR will be offered and hence performed. Until then, the TABASC is unable to confirm what, if any, technical smart metering changes may be needed.

[This section to be further updated post SSC meeting]

3. Common Systems – Communication Networks

Dependent on the security requirements, and risk assessment to be completed, the Panel recognises the potential synergy benefits for wider industry, by amending the DCC licence to provide a common and secure platform for communications. However, in making any amendments to the DCC Licence, and the scope of the services the DCC provides, a review of the cost recovery for these new services under the SEC must be undertaken. Such a review should ensure that the users of those new services, contribute to the DCC design, build and ongoing service costs for the new service provision.

Public Key Infrastructure (PKI) and Anomaly Detection Thresholds (ADT) is familiar to industry, as this forms part of the security solution for smart metering communication via the DCC. The SEC Panel, DCC and SECAS are very familiar with issues with managing security standards, PKI and ADT. The SEC is a natural fit to govern this requirement.

4. Delivery Framework

The Smart Metering Implementation Programme (SMIP) has been working in tandem with SEC for several years, with work transitioning from SMIP to enduring SEC governance, as services mature. The delivery framework proposed in the consultation is therefore familiar and is a model the SEC Panel and SECAS would be comfortable operating within.

Future development of the SEC under Option 2 discussed in the consultation, to encompass a delivery framework for ESA and DSR regulations, would provide industry with a single place within which all “smart” devices are managed. For example, new schedules and sections may be added to the SEC, to

detail the services provided and requirements for industry compliance, to facilitate the expected growth of this area of the market. Learning may be applied from the SMIP and SEC Panel from incorporating and managing newly designated sections of the code, and development of appropriate governance and oversight.

The Panel is keen to work closely with BEIS to further develop and discuss ways in which the Panel and the SEC governance framework may facilitate the growth of this important market sector.

If you would like to discuss any aspects of this response further, please do not hesitate to contact me on 020 7090 7755 or SECAS@gemserv.com

Yours Faithfully,



Peter Davies
SEC Panel Chair

DRAFT