Department for Business, Energy & Industrial Strategy

Department for Business, Energy & Industrial Strategy
1 Victoria Street
London SW1H 0ET
www.gov.uk/beis

The Authority (Ofgem), the SEC Panel, SEC Parties and other interested parties

26 March 2020

Dear Colleague,

CONSULTATION ON THE EXTENT TO WHICH THE ENDURING CHANGE OF SUPPLIER ARRANGEMENTS SHOULD BE SEPARATED FROM OTHER ARRANGEMENTS UNDER THE SMART ENERGY CODE

This consultation seeks stakeholders' views on the extent to which the Systems and other arrangements applying in relation to Enduring Change of Supplier (ECoS)[1] should be required to be separated from other Systems and arrangements in place under the Smart Energy Code (SEC) in order to ensure robust security.

We are not, at this stage, consulting on the specific legal drafting changes that would be required to give effect to these proposals, but instead upon the principles that would apply to the separation in order to advise DCC's procurement process. We plan to consult on the legal drafting changes at a later stage once the full scope of the changes needed to support ECoS are known.

The consultation document giving details of the proposals, and how to respond ahead of the closing date of 7 May, is in the Annex to this letter.

Yours faithfully,

Duncan Stone
Deputy Director & Head of Delivery
Smart Metering Implementation Programme

Annex: Consultation document

[1] The Enduring Change of Supplier arrangements are changes to the process that the DCC follows when a consumer changes energy supplier and the new supplier seeks to take over control of the Smart Meter and other Devices in the consumer premises. They replace the existing "Transitional Change of Supplier" processes that were originally implemented and which were intended to be temporary. More information on the DCC's plans to deliver the necessary changes can be found here: https://www.smartdcc.co.uk/customer-hub/consultations/consultation-on-the-delivery-plan-for-enduring-change-of-supplier/

Annex: Consultation document

1. Table of Contents

2. General Information

Why we are consulting

This consultation seeks stakeholders' views on the separation arrangements that should apply to the systems that are used to support the Enduring Change of Supplier (ECoS) arrangements that are to be put in place under the Smart Energy Code. It is intended that the arrangements would advise DCC's procurement process and ultimately the legal drafting changes to support ECoS which are planned to be consulted upon at a later stage once the full details of the necessary changes are known.

Timing

Responses to this consultation should be submitted by 17:00 on 7 May 2020.

Responding to the consultation

Your response will be most useful if it is framed in direct response to the questions posed, by reference to our numbering, though further comments and evidence are also welcome.

Responses should be submitted to smartmetering@beis.gov.uk

When responding, please state whether you are responding as an individual or representing the views of an organisation.

Confidentiality and data protection

Information you provide in response to this consultation, including personal information, may be disclosed in accordance with UK legislation (the Freedom of Information Act 2000, the Data Protection Act 2018 and the Environmental Information Regulations 2004).

If you want the information that you provide to be treated as confidential please tell us but be aware that we cannot guarantee confidentiality in all circumstances. An automatic confidentiality disclaimer generated by your IT system will not be regarded by us as a confidentiality request.

We will process your personal data in accordance with all applicable UK and EU data protection laws. See our privacy policy.

We will summarise all responses and publish this summary on the SECAS website. The summary will include a list of names or organisations that responded, but not people's personal names, addresses or other contact details.

Territorial extent

This consultation applies to the gas and electricity markets in Great Britain. Responsibility for energy markets in Northern Ireland lies with the Northern Ireland Executive's Department for the Economy.

Quality assurance

This consultation has been carried out in accordance with the government's consultation principles.

If you have any complaints about the way this consultation has been conducted, please email: beis.bru@beis.gov.uk.

3. Existing Separation Requirements

Background

1. When a consumer switches energy supplier, the security information held on the Smart Meter needs to be changed so that it relates to the new energy supplier and not the old one. The processes that are currently in place for managing the change of security information held on Smart Meters are referred to as the "transitional change of supplier" processes and are administered by part of the DCC Systems known as the "change of supplier party" or "CoS Party"[2].

2. In addition to storing security information about the energy supplier for the premises, Smart Meters also store security information about the CoS Party. When a command is sent to a Smart Meter to change the energy supplier's security information, the Smart Meter checks that the command has been sent via the CoS Party and that the CoS Party has warranted that the new security information is that of the incoming supplier, and that that information has not been altered in transit. Only when the meter has successfully applied these checks will it replace the old energy supplier's security information with that of the new one.

3. In addition to the checks applied by the CoS Party when processing requests to change energy supplier security information on Smart Meters, other parts of the DCC's Systems carry out other security checks on commands before they are sent to Smart Meters. The Systems that apply these other checks are known as the "Access Control Broker" (or "ACB") Systems[3].

Existing Separation

4. The CoS Party Systems and ACB Systems each carry out important security checks on commands that are to be sent to Smart Meters, all of which need to be passed before the commands are sent. From a security perspective, it is important that these two Systems are kept separate so that there are separate safeguards to defend against any would-be security attacks. The Smart Energy Code (SEC) sets out the requirements that dictate the extent to which these two Systems (and other parts of DCC's Systems and User Systems) need to be separated. For example, the DCC is required to put controls in place to ensure that any information exchanged between the CoS Party and the ACB is for a necessary purpose. It also imposes restrictions that: either prevent the same person from being given access to both Systems if that person's level of access is such that they could cause a compromise of the Systems; or if the same person is given such access, that additional controls are in place to prevent their actions from causing a material compromise of any of the Systems.

[2] The existing CoS Party Systems are referred to as the Transitional Change of Supplier Systems (TCoS Systems) whereas the replacement CoS Party Systems will become the Enduring Change of Supplier Systems (ECoS Systems).

[3] More specifically, these Systems form limb (b) of the definition of DCC Live Systems under the SEC.

4. Proposed Enduring Change of Supplier Arrangements

Background

5. As their name suggests, the existing transitional change of supplier processes were intended to be temporary. Changes to replace the existing transitional change of supplier arrangements to the enduring solution are already underway. Following a direction issued by the Secretary of State under condition 13A of the DCC licence, on 23 January 2020 the DCC published a consultation on its draft plan[4] for its delivery of the enduring change of supplier arrangements.

6. In parallel with publishing its draft condition 13A plan, the DCC has mobilised its project to implement the ECoS arrangements and is seeking to issue tenders for organisations to deliver systems to support the new arrangements. In order to inform these procurements and in advance of the changes to the SEC that are needed to support the ECoS arrangements having been fully developed, BEIS has given further consideration as to the degree of separation that should be required between the ECoS Systems and other parts of the DCC Systems, particularly those of the ACB.

7. This document is a consultation on those proposed separation requirements. As discussed above, it is intended that the results of this consultation may be used to inform the DCC's procurement process and will ultimately be reflected in SEC drafting.

Proposed Separation Requirements

8. We are proposing that a number of separation requirements should apply between the ECoS Systems and other parts of the DCC Systems. In the SEC, the various parts of the DCC Systems that are required to be separated from each other form different limbs of the definition of DCC Live Systems. For example, the ACB Systems constitute limb (b) of this definition, whereas the CoS Party Systems (which will become the ECoS Systems) constitute limb (c).

9. Other than where specific exceptions apply, Section 2.20 of Section G of the SEC requires each limb of the DCC Live Systems to be "Separated" from each other. The concept of "Separated" is defined in the SEC, and, as described above, essentially means that the DCC must implement controls to ensure that information flowing between any Separated Systems is for an intended purpose.

10. We are proposing that this existing Separation requirement should be retained and apply to the ECoS Systems. This means that the ECoS Systems would be required to be Separate from all other limbs of the DCC Live Systems (as well as, for example, being Separate from User Systems).

11. We are also proposing that, as between the ECoS Systems and the ACB Systems, the following additional Separation requirements would apply:

    (i) where either of these two Systems receives information purporting to come from the other System, then it should be capable of verifying that the information has originated from the other System and that the information has not been modified after having been sent;

[4] https://www.smartdcc.co.uk/media/3543/consultation-on-the-delivery-plan-for-enduring-change-of-supplier.pdf

(ii) the DCC shall ensure that personnel (including those of DCC and any working on behalf of any External Service Provider) are appropriately segregated such that no individual is capable of introducing a security vulnerability into both Systems;

(iii) no person that is involved in the development or customisation of bespoke firmware or software on one of these two Systems within the past 24 months[5] (or such shorter period of time as may be approved by the Security Sub Committee) may be involved in the development or customisation of bespoke firmware or software on the other System;

(iv) no person may be a Privileged Person in relation to one of these two Systems if they are or have been a Privileged Person in relation to the other System (provided that if they have ceased to be a Privileged Person in relation to one of the Systems, they may be a Privileged Person in relation to the other after a period of not less than 6 months[5] after that cessation has elapsed);

(v) the DCC must ensure that External Service Providers of the two Systems are corporately separate at all times. This means that External Service Providers for one System cannot be Affiliates or Related Undertakings[6] of External Service Providers of the other System;

(vi) in addition to the above, the DCC must ensure that:

a. where a provider of the ECoS Systems has (or comes to have) an Ultimate Controller, (a holding company of the provider of the ECoS Systems that is not itself a subsidiary of another company) the ECoS provider must procure a legally binding undertaking from the Ultimate Controller (which is enforceable by DCC) confirming that it will ensure the required corporate separation is maintained;

b. the ECoS contract(s) with DCC oblige(s) the ECoS service provider(s) to ensure that the required corporate separation is maintained; and

c. the ECoS contract is such that any breach of the obligations referred to in (a) or (b) is an event of default under the contract entitling DCC to do one or more of the following: (i) require divestment so that the corporate separation is re-established; (ii) terminate the ECoS contract and/or (iii) recover the DCC's costs arising as a direct result of the event of default including any fines or re-procurement costs.

12. The first of these additional separation requirements is intended to ensure that cryptographic checks are implemented to assure the origin and integrity of information exchanged between the ECoS Systems and ACB Systems.

13. The second, third and fourth requirements are aimed at providing additional organisational separations that apply between ECoS Systems and ACB Systems by placing restrictions on personnel that are involved in their design, development and operation, where such personnel could have an influence over the security of either of the Systems.

14. The fifth and sixth requirements are aimed at ensuring that no single person or organisation can control both ECoS Systems and ACB Systems, both when the Systems are procured and on an ongoing basis. We do not believe these two requirements would be costly to implement in practice as they would form part of the DCCs re-procurement requirements for these aspects of the ACB and ECoS. They simply require ECoS service providers to first, not be an Affiliate or Related Undertaking

[5] We are seeking to strike a balance between preventing any individual from having an opportunity to introduce a vulnerability into both Systems and not unduly preventing those with relevant expertise from providing services to DCC. Views are specifically invited on the duration of these periods.

[6] By "Affiliates" and "Related Undertakings" we mean the terms as currently defined in the DCC Licence.

of providers of the ACB Systems and second, to procure a legally binding undertaking from their Ultimate Controller that they will not (for example through corporate mergers, acquisitions, sales, etc.) take any steps that means that the separation requirements are no longer met.

15. We are also proposing that any independent security testing of either system that is used to provide assurance must be carried out by an organisation that is a CHECK[7] service provider and is not a company that designed or developed either System, nor is it an Affiliate or Related Undertaking of those which have designed or developed either system.

16. We are not proposing a specific obligation on DCC to split the security testing of the ECoS and ACB Systems between different organisations, but have an expectation that there will be periodic rotation in the organisation(s) that are used to carry out such testing as part of best practice in this area.

17. We have discussed these separation proposals with the Security Sub Committee and DCC, and indeed they incorporate changes that we have made in light of the helpful comments that were provided on our initial proposals. In light of these discussions, we understand that the Security Sub Committee, the Technical & Business Design Group and DCC are broadly supportive of the proposals.

5. Consultation Questions

1.	Do you agree with the proposed additional Separation requirements?
2.	In particular, do you have any views on the appropriateness of the 24 month and 6 month restrictions proposed in the separation requirements? Please provide an explanation of any views you have.

[7] CHECK is the scheme under which companies approved by the National Cyber Security Centre can conduct authorised penetration tests of public sector and Critical National Infrastructure systems and networks.