SCOTTISHPOWER

Smart Metering Implementation Programme
DECC
55 Whitehall
London
SW1A 2EY

26 July 2012

Dear Sir/Madam,

SMART METERING – REQUEST FOR COMMENTS ON LICENCE CONDITIONS RELATING TO SECURITY RISK ASSESSMENTS (PRE-DCC PERIOD)

Scottish Power is pleased to respond to the Government's consultation dated 31 May 2012 on smart metering and the proposed licence conditions relating to security risk assessments and audits in the remaining period prior to DCC go-live.

Our answers to the consultation questions are in Annex 1 attached. Our main points relating to this consultation document are as follows:

- **Legal powers:** Section 88(1) of the Energy Act 2008 is limited by section 88(2) to the purpose of [provision, installation or operation] of [compliant smart meters]. It seems to us that this limits the provisions to security for SMETS compliant smart meters and not other ADMs which may be being rolled out at the same time. Similarly, it is not clear that the power to require licence holders to "make arrangements" for related matters can include the direction powers envisaged.

  We would suggest that care is taken to stick within the powers set out; if they prove too narrow, Ofgem could introduce licence changes using its general powers.

- **Supplier obligations:** If DECC is to deliver its intended security objective there can be no difference in security standards for large and small suppliers. A breach of security would be damaging for consumer confidence whatever size of party it comes from. Any mitigation of requirements for parties with a small number of smart meters should be limited to peripheral areas which do not affect the security standards to be employed. This could be achieved by giving the Authority a power to grant derogations from particular requirements where it is satisfied that security would not be put at risk.

  In order to fully assess the intended smart metering security standards, it would be helpful to have a more detailed understanding of the intended enduring security requirements, briefly referenced in the consultation document. In addition, suppliers will require a full understanding of the assurance and accreditation requirements, and the intended DCC enrolment and adoption criteria if they are to work effectively and consistently towards DECC's intended enduring security obligations in the lead up to DCC go-live.

- **Application of ISO27001:** Further consideration of the interpretation and application of security standard ISO27001:2005 is required. A detailed assessment of the standard should be carried out to determine the practices that suppliers already have in place and ensure that suppliers and the Authority have a common understanding of how the standard is to be implemented across the industry in the context of smart metering, and how compliance will subsequently be audited.

  We are also concerned that unduly elaborate interim measures could detract from the main focus of achieving DCC go live and commencing mass roll out in 2014.

- **Timescales:** Further consideration should be given to the practicalities of individual parties achieving the appropriate level of compliance within 6 months of the proposed licence condition coming into force. We feel that a timeframe of at least 9 months would be more appropriate, taking into account the activities which would need to be undertaken - including the appointment of a qualified organisation and subsequent initial audit which could include an element of remedial activity.

- **Authority/Secretary of State directions:** We strongly recommend that the Part D provisions for the Secretary of State and/or the Authority to give suppliers specific directions are removed from the licence conditions. We think they are wrong in regulatory principle since they confuse the tasks of regulation and management and raise questions of liability if compliance with the direction causes any loss or injury. There is no explicit obligation on the directing party to consult with the licensee or to satisfy itself that it is reasonably practicable (and proportionate) for the licensee to comply. We also have doubts as to whether such a power is within the *vires* of section 88(1) of the 2008 Act and believe that the remainder of the condition plus Ofgem's enforcement powers are sufficient.

- **Transition from pre-DCC to enduring security arrangements:** While there may be initial timing issues, we would expect enduring security requirements to be included in the Smart Energy Code (SEC). Based on drafting within the consultation document, we would be grateful for further clarification with regard to the security requirements for meters which continue to be operated outside the DCC post go-live.

Our review of the consultation document and the proposed licence conditions has to a degree been limited by the absence of detailed enduring security requirements. While we note DECC's intention that these will be published shortly, their availability would provide a better context in which to assess the measures DECC is proposing in the interim period. However, in addition to considering the licence conditions we have also proposed drafting changes which are primarily outlined in our response to Question 1.

Should you wish to discuss any areas of this initial response in more detail, please do not hesitate to contact me using the details above o

Yours faithfully,

Annex 1

Question 1: Do you consider that the draft licence conditions deliver the policy intention outlined in this document? Please provide comments on where the drafting could be amended or clarified.

The draft licence conditions appear to reflect the policy intention outlined in the consultation document. However we feel that further consideration should be given to the interpretation and application of the security standard ISO27001:2005 referenced in Z.8. An assessment of the security standard should be carried out to determine the measures that suppliers already have in place and ensure that suppliers and the Authority have a common understanding of how the standard is to be implemented across the industry, in the context of smart metering, and how compliance to the standard will subsequently be audited.

We agree that it is necessary for all suppliers to undertake appropriate security risk assessments to ensure that a consistent level of security assurance is achieved across the GB smart metering estate. However, in the period leading up to DCC go-live we would question the level of prescription, noting that suppliers are already subject to measures under the Supplier Volume Allocation Qualification process and Performance Assurance Framework which does not specify alignment to ISO27001. Auditable sections within the Self Assessment Document do however address operational security and controls, change management and risk assessment – prerequisites of entering and subsequently operating on within the market on an on-going basis. We are also not aware of industry parties such as network operators, responsible for critical national infrastructure, being subject to such specific standards.

In respect of the drafting of the proposed licence conditions, we make the following observations:

- **Z.1** – we note that the condition refers to "Smart Metering Systems". There is no definition of such in the condition but elsewhere it is defined as SMETS compliant meters and we think this is intended here. We think this is correct; there are no *vires* to extend this condition to other ADMs.

- **Z.2** – makes reference to 'SEC Go Live'. We believe that this should be changed to 'DCC Go Live' on the basis that in the Smart Metering Implementation Programme's current plan, the SEC Go Live milestone is aligned with DCC licence award in Q2 2013.

- **Z.2** – we believe that the licence condition ceasing to have effect at the point of SEC Go Live (DCC Go Live – see above) requires further clarification with regard to those meters which continue to be operated outside the DCC post-DCC go-live.

- **Z.4** – this should have some concept of taking all reasonable steps. Otherwise the condition could require the devotion of infinite resources to security.

- **Z.5** – the components of the end-to-end system do not match those listed in section 3.6 of the consultation document. If it is the intention that the scope of the end-to-end system includes a supplier's head-end system and all business procedures associated with the installation, operation and support of the system, the missing elements which are listed in section 3.6 will need to be included in Z.5.

- **Z.5** – it is evident that the supplier is in no position to prevent the customer from interfering with the meter; the best that can be hoped for is to make it difficult and detectable. Since this paragraph defines the meter as something which must be made secure, there will need to be exclusions in Z.6 which indicate that the supplier has limited duties to prevent interference by the customer.

- **Z.6** – the cross reference in line 1 should we think be to Z.4

- **Z.8** – We would suggest that the concept in the consultation document would be more closely captured by "to the extent reasonably practicable, implement security procedures that are consistent with the following standards..."

- **Z.10** – suppliers are in no position to control who has physical access to the meter in the customer's home. There needs to be an exclusion in subparagraph (b) accordingly.

- **Z.14** – the proposal that suppliers must conduct their first audit within 6-months of the licence condition coming into force presents a significant challenge. The practicalities of achieving compliance within the timeframe should not be underestimated. Within the six-month period activities would need to include:
    - appointment of a qualified organisation to undertake the audit;
    - putting in place the necessary arrangements for the first audit to be completed (which may include appropriate access to third parties); and
    - Implementing any necessary remedial actions.

  We would therefore propose that undertaking the first audit within 6-months of the licence condition coming into force is too short and would recommend that the timeframe is extended to at least 9 months. This consideration should form part of the assessment exercise we propose above

- **Z.14** – While the definition of a Competent Independent Organisation (CIO) and their relevant accreditation qualifications is covered under Z.20, the current definition does not specify whether the audit should be undertaken by an accredited individual. In order to remove any ambiguity we would propose that audits can only be undertaken by accredited individuals employed by a CIO.

- **Z.17** – This should be deleted. We think the powers of specific direction are wrong in regulatory principle since they confuse the tasks of regulation and management and raise questions of liability if compliance with the direction causes any loss or injury. There is no explicit obligation on the directing party to consult with the licensee or to satisfy itself that it is reasonably practicable (and proportionate) for the licensee to comply. We also have doubts as to whether such a power is within the *vires* of section 88(1) of the Energy Act 2008 and believe that the remainder of the condition plus Ofgem's enforcement powers are sufficient.

We also note that there is inconsistency in the drafting of the consultation document with reference to the scope of security arrangements being 'all smart metering systems' (section 2.4) and 'SMETS meters deployed during the pre-DCC go live phase (section 4.1). We do not think that the powers in section 88(1) of the 2008 Act include non-SMETS meters.

Question 2: Do you have any comments on the proposed approach that suppliers should carry out a number of good practice security disciplines and procedures as is set out in this document?

We acknowledge that the ISO27001 security standard is widely recognised as a measure of best practice. But given that suppliers are already operating Advanced Domestic Meters without the need for such regulation, we propose that DECC should undertake a detailed review to check that the standard can be effectively and proportionately applied to smart metering.

The interpretation and application of ISO27001 must be consistent across all affected parties. A key objective of the proposed review should be to identify areas where additional guidance is necessary including the audit process. Any differences in interpretation could lead to inconsistency across the industry which would defeat the intentions of specifying a specific standard and could lead to further re-work by affected parties or the Authority.

All suppliers should be subject to the same levels of security rigour. Placing a single objective on all parties, irrespective of their organisational size, customer base or number of smart meters deployed will ensure that DECC achieves one of its key objectives around the security of the end to end smart metering system. Such an approach will also ensure appropriate assurances can be passed on to the end user – the consumer.

Question 3: Do you have any further comments with regard to the issues raised in this document? We also welcome general comments around the approach to small suppliers, the processes expected of suppliers in general, and any related costs.

Combined assessment of interim and enduring requirements

In order to fully assess the intended smart metering security standards, we ideally require a detailed understanding of the intended *enduring* security requirements, briefly referenced in the consultation document. In addition, a full understanding of assurance and accreditation requirements in conjunction with the intended DCC enrolment and adoption criteria is necessary if suppliers are to work effectively and efficiently towards DECC's intended enduring security obligations.

While the consultation document suggests a framework by which individual suppliers can move towards ISO27001 in the remaining period leading up to DCC go-live, current requirements could still be subject to significant change – including conclusion of SMETS and final selection and ownership of communications technology and devices. The proposed interim arrangements will also need to be assessed against the potential redistribution of roles and responsibility once the DCC is in place.

We believe that a detailed review of ISO27001 in the context of smart metering should be carried out to ensure that suppliers and the Authority have a common understanding of supplier obligations and the required approach to compliance auditing. This would minimise the risk that suppliers will need to re-visit or seek re-audit of their security arrangements as a result of inconsistencies in interpretation and application. However, this risk cannot be fully mitigated if suppliers are expected to put in place arrangements while the enduring end to end architecture and associated roles and responsibilities are still to be finalised.

Equal supplier security standards

As stated in our response to Question 2, we do not believe there should be different security standards for large and small suppliers. All parties, irrespective of their organisational size,

customer base or number of smart meters deployed should be subject to the same security standards. If this approach is not followed, there will be the potential for inconsistencies across the industry which would ultimately defeat DECC's intentions set out in this consultation document. As DECC notes, '*A failure or oversight of a security control in one element of the system could undermine the overall security solution.*'[1] Without a consistent approach to security across all affected industry parties, the Government will be unable to provide the necessary assurances to key stakeholders.

Transition from pre-DCC to enduring security arrangements

While the consultation sets out DECC's intended security framework and underpinning standard pre-DCC, it raises further questions with regard to the transition from pre-DCC to enduring arrangements. We would welcome clarification in this area, with the expectation that the status of non-SMETS compliant meters (and variations of SMETS compliant meters which continue to operate out with the DCC post go-live) will be confirmed in the subsequent enduring smart metering security requirements consultation.

ScottishPower
26 July 2012

[1] Condoc page 6, para 2.1