energyuk

Smart Metering Implementation Programme

Consultation on a draft licence condition relating to security risk assessments and audits in the period before the DCC provides services to smart meters

A Response from Energy UK:

Executive Summary

Energy UK is the new trade association for the gas and electricity sector, representing a wide range of interests and driving forward the debates on the UK's strategy for achieving a low carbon, secure and affordable energy future. It includes small, medium and large companies working in electricity generation, energy networks and gas and electricity supply, as well as a number of businesses that provide equipment and services to the industry. Energy UK welcomes the opportunity to respond to this consultation.

Whilst Energy UK fully supports the need for security arrangements during the Foundation stage of the programme, our members have noted that the consultation is limited by the absence of enduring security standards. Therefore if suppliers are expected to work towards achieving certification by DCC Go Live, a full understanding of the overall security framework would be beneficial, the sooner that levels of certainty can be given, the sooner businesses can prepare with some comfort that they can minimise costly rework. It must be recognised that assuring adequate and consistent security is neither straightforward nor inexpensive.

Many of our members also believe that an understanding of the enduring assurance and accreditation arrangements as well as the intended DCC enrolment and adoption criteria is necessary to ensure suppliers work effectively and consistently towards enduring security requirements.

Summary of key points:

- Obligations should apply to all suppliers – there should be no difference in security obligations for large or small suppliers. If a standard approach is not taken, there will be the potential for inconsistencies across the industry ultimately defeating the intentions set out in the consultation.

- Obligations need to be applied fully appreciating the impact they cause– security must continue to be fit for purpose, but the approach to achieving that must be proportionate and pragmatic. Energy UK would appreciate assurance that this will be the approach.

- Application of ISO27001 – further consideration of the interpretation and application of the security standard is required. Detailed assessment will determine the practices that suppliers already have in place and that an equal understanding of how the standard should be implemented and audited across the industry.

- Timescales – the practical challenges for all suppliers implementing the obligations and achieving the same level of compliance within the suggested 6 month timescale is unreasonable.

- The ability for the Authority to issue directions – it is unclear from where the Authority will take advice in making decisions to issue directions. Energy UK would wish to be assured that the advice is sound and that any direction results from full and pragmatic consideration of the risks, options and impacts.

- Transition – further clarity is required in relation to the security requirements for meters which are either SMETS non-compliant or continue to be operated outside the DCC. The change of supplier process will also need consideration.

Consultation Questions:

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

Energy UK Response:
Overall, Energy UK's members all agree that the draft licence conditions do deliver the appropriate policy for security requirements required for the Foundation period of the programme. It is wholly appropriate and necessary for all suppliers, large and small, domestic and non-domestic, to have undertaken appropriate security risk assessments for any smart or advanced meters installed prior to the DCC go-live date. In setting out clear obligations on suppliers as specific licence conditions, there should be no ambiguity or room for differing interpretation of obligations, and this will give all suppliers the required assurances needed that any advanced or smart meter they inherit has gone through the same level of risk assessment as their own.

However, neither the consultation document itself, or the proposed licence conditions provide the necessary clarity in relation to the types of meters expected to be covered by the security obligations. In section 2.4, the reference is "all smart metering systems", yet in section 4.1, the reference is "SMETS meters deployed during the pre-DCC 'go-live' phase". This inconsistency needs clarifying urgently, and Energy UK would recommend that Government writes to all relevant stakeholders to confirm its policy intentions as soon as is practically possible.

Not only do we need clarity on the types of meters, we require certainty on the security requirements that suppliers are expected to assess against. The latest publication of security requirements is v0.5 and suppliers are generally assuming that this is the baseline to consider for SMETS1 meters. It would be helpful if this was published as a finalised baseline (e.g. 1.0) and the SMETS version that it applies to explicitly referred to (e.g. SMETS1). Any future versions of the security requirements will need to be assessed against the SMETS and associated systems/processes extant at the time.

In terms of specific aspects of the drafting of the licence condition, Energy UK has the following observations to make:-

- Z.2/Z.3 – refers to "SEC Go Live". For clarity, our members believe that the reference here should be "DCC Go Live". It is our understanding that the SEC will actually go live at the point that the DCC licence award takes place, although at that point, the SEC will be a very light document setting out only basic governance arrangements rather than including detailed requirement and obligations on users of DCC's services.

- Z.2 – The intention for the licence condition to cease to have effect at the point of SEC Go Live (see Energy UK's comments in point one above – our members agree that this should be DCC Go Live) does raise the question as to what arrangements will be needed for those meters that do not comply with SMETS (v1 or v2), or those that do comply with SMETS but are not enrolled within the DCC after the DCC Go Live date. Energy UK has noted the intention for the programme to further consider what the appropriate assurance regime should be for those meters operated outside of the DCC and what any transitional arrangements may be necessary .

- Z.4/Z.5 – The categories of the End-to-End systems explained in Z.5 do not reflect the expectations as set out in paragraph 3.6 of the consultation document itself. In paragraph 3.6, there is an expectation that the End-to-End system includes the supplier's head end system and all of the business procedures associated with the installation, operation and support of the system. If the general duty to ensure a secure End-to-End system includes a supplier's internal business procedures as described in paragraph 3.6, then this should be reflected in the categories described in Z.5. There needs to be certainty on how far into the supplier's organisation, systems and processes security requirements are expected to be complied with.

- Z.14 – Energy UK's members have expressed initial concern with the suggestion that the licensee must conduct its first audit within 6 months of the licence condition coming into force. Whilst suppliers have sufficient insight into what obligations they will be required to comply with, the practicalities of appointing a suitably qualified organisation to undertake the audit, and to put in place all of the necessary arrangements to carry out the initial audit, all within a 6 month period will be challenging. Energy UK's members believe that the requirement to carry out the initial audit should be extended to at least 9 months to allow the appropriate arrangements to be put in place.

- Z.14 – The draft licence condition requires audits to be carried out by a Competent Independent Organisation (CIO). Whilst the definition of a CIO under Z.20 clarifies the relevant accreditation requirements for the CIO itself, the current definition suggests that audits do not have to be carried out by accredited individuals. Instead, the current definition (that an organisation qualifies as a CIO if it employs just one consultant who is a member of the CESG Listed Advisor Scheme) would allow audits to be carried out by anyone employed by the organisation. Energy UK's members believe that in the interests of removing any ambiguity in this area, audits should only be carried out by properly accredited individuals.

- Z.17 – Whilst Energy UK's members support the ability for the Authority to issue direction to take (or refrain from taking) steps as may be set out in any such direction, the consultation does not set out where the Authority is taking advice from in setting any such directions. Whilst such detail is not necessary for licence conditions themselves, Energy UK's members believe Government should confirm whether it is the intention for the Authority to be informed by the current Security Technical Expert Group established under the SMIP, or whether it envisages the Authority will set up its own advisory group. Energy UK's members all agree that in setting any such direction/s, the Authority must carry out an appropriate cost benefits exercise so that all parties affected can be assured the actions being proposed are both relevant and proportionate to the associated risk, and necessary in the timescales being proposed in any direction/s.

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 set out in this document?

Energy UK Response:
Energy UK's members are broadly supportive of the approach proposed. Our members agree with the suggestion that ISO 27001 appears to be the most relevant standard to which suppliers should be aiming to achieve. Whilst suppliers are familiar with ISO 27001, it has been suggested that it may be appropriate to carry out an overall review of the standard to confirm that it is wholly relevant to smart meters and any associated business processes that are likely to be impacted by them. Our members all agree that in order for security obligations to deliver the needed assurance to industry, to Government (and the Authority), and to all relevant stakeholders, there needs to be a consistent application of the standard across all parties, and a consistent process for the Authority to assess suppliers' compliance with the proposed licence obligation.

With this in mind, the review should seek to highlight any areas of the standard that might benefit from some additional guidance when suppliers are putting place the necessary arrangements, especially in terms of audit. Any instances of differing interpretation or any inconsistency could defeat the overall objectives of specifying a specific standard in the first place. A key example where clarity can be provided is the Security Requirements – for that reason we propose that the Smart Metering Security requirements (currently v0.5 and marked as draft) be baselined to version 1.0. This document can then formally be regarded as part of the security product set against which all suppliers can have confidence to reference.

As noted in our response to question 1 above, Energy UK's members all agree that the proposed obligations must apply to all suppliers consistently, regardless of their size, numbers of customers they supply, and equally to suppliers of non-domestic customers that could theoretically be enrolled into the DCC once operational. Energy UK's members believe that by placing the obligation on all suppliers, Government can deliver its objective of ensuring that the end-to-end smart metering systems that suppliers manage and operate are adequately secure, ultimately providing the necessary assurances to all parties including end-users.

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.

Energy UK Response:
As indicated in our response to Question 1 above, Energy UK's members all expect the enduring security requirements and obligations to be included within the SEC. Consideration is therefore required in relation to the transition from the proposed licence obligations ceasing to take effect, and the new security requirements and obligations under the SEC coming into force.

Energy UK's members all support the need for a review of the ISO 27001 standard, and if appropriate, to develop a set of guidance notes to sit alongside the proposed licence conditions. This review should also take into account the different roles and responsibilities of the various owners of components of the end-to-end smart metering system, and against the roles and responsibilities of parties expected for the Enduring stage including those of the DCC so that suppliers can fully understand the level to which interim measures might need to fall away once we arrive at DCC Go Live.

It is vital that wherever possible, all suppliers (as part of developing and implementing their security arrangements), and the Authority (in terms of assessing compliance against the proposed licence obligations) have a consistent understanding of the definitions and requirements being proposed and obligated. Without this consistency, there is a risk on suppliers that when acquiring a new customer with a smart meter installed, they could inherit a smart metering system that has not gone through the same level of security assessment expected. This guidance should also remove or reduce the risks of the need for suppliers to revisit or re-audit their security arrangements if inconsistencies in interpretation are uncovered (either by suppliers themselves, or by the Authority) at a later date.

As indicated previously in this response, Energy UK's members all agree that the proposed obligations for security must apply to all suppliers regardless of their size, or segment of the market they operate in. Whilst carrying out risk assessments for security should form part of any suppliers' implementation plans, setting out firm obligations on all suppliers in this manner should help provide the appropriate assurances to all stakeholders that adequate security protections are in place to protect not only the associated infrastructure and equipment, but also the messages and data being transmitted.