Smart Metering Implementation Programme
Department of Energy and Climate Change
Room M09
55 Whitehall
London SW1A 2EY
26th July 2012

Consultation on a Draft License Condition Relating to Security Risk Assessments and Audits in the Period Before the DCC Provides Services to Smart Meters

Dear SMIP Team,

Thank you for the opportunity to respond to this consultation.

At a high level we would like to make four points:

We believe that security is one of the cornerstones of the smart metering programme. As has been seen around the world, smart metering systems and smart grids are being targeted more and more by individuals and organisations with malicious intent, and we wholeheartedly agree that the UK smart metering roll out must be secure.

The customer is at the heart of the smart metering programme, and this licence must above all protect the customer and their supply of energy. We would strongly support a licence environment in which all suppliers can mutually trust each others' security implementations to avoid the possibility of having to revert the meters of gained customers to a non-smart state.

We believe that all organisations in the smart programme should be held to the same standards, to ensure that customers enjoy at least the same minimum standard of security irrespective of supplier.

The smart metering roll out in the UK is still at an early stage. It is inevitable that some aspects of the programme's security model will change as a result of experience acquired during rollout. We acknowledge that there needs to be a way to put directives forward to the various licence signatories, however we believe that this should be the role of the Authority as they are responsible for compliance with the licences.

Yours sincerely

RWE npower

Trigonos
Windmill Hill Business Park
Whitehill Way
Swindon
Wiltshire SN5 6PB

T

Registered office:
RWE Npower plc
Windmill Hill Business Park
Whitehill Way
Swindon
Wiltshire SN5 6PB

Registered in England
and Wales no. 3892782

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.

In general we agree that the licence conditions reflect the policy intent, however neither the policy intent nor the licence conditions specify whether these conditions are to become part of an existing licence (and if so which one(s)) or if a new licence is to be created. Due to the time constraints we would expect these conditions to be amendments to an existing licence condition that is already in effect. We are also concerned that the draft licence conditions refer to the Smart Energy Code, however based on the announced timescales of the two sets of licence conditions, the Foundation Security licence may well come into force before the Smart Energy Code that it references.

There is no mention of whether these licence conditions only apply to domestic meters, or if they are expected to apply to non-domestic meters as well. Our current expectation is that many non-domestic smart meters will remain outside of the DCC for the whole of their lifetimes. Consideration should therefore be given to the implications of a Supplier License Condition that is proposed to expire at the point of DCC go live. We believe that this would fail to protect those customers with smart meters that are compliant in terms of rollout but which will continue to be managed outside of the DCC. This will apply to non domestic customers, where use of the DCC is optional and also to domestic customers with SMETS1 meters that may no be adopted by the DCC.

We believe that the following statements in the draft licence conditions require rewording or alteration in order to more accurately reflect the policy intent:

- Z.3 – The licence conditions refer to the "SEC Go Live" date from the Smart Energy Code, however there is no "SEC Go Live" date in the SEC. There is the date the SEC comes into effect, and the "DCC Go-Live" date. The commentary makes it clear that it is the DCC Go-Live date, but the licence is ambiguous and should be changed to reflect the "DCC Go-Live date"

- Z.7: We believe that the documented evidence mentioned in this statement should be presented to the Authority rather than the Secretary of State. The Authority is responsible for ensuring compliance with all licence conditions and as such is the appropriate party to hold and inspect any such evidence.

- Z.8 We believe that the phrase "must take reasonable steps to ensure that it is able to comply" is too vague. This phase can be interpreted as "an organisation must be able to say it would be able to comply if it wanted to", not that it actually can comply. The wording should be changed to "must take reasonable steps to comply" in order to more accurately reflect the policy intent and to remove the ambiguity.

- Z13.a: The reference to "Staff" should be replaced with something more generic that also covers individuals on short term contracts and third party organisations. It may be that a third party specialist firm is brought in to perform the work. We would suggest that the wording be changed to: "commit sufficient appropriately qualified resources to ensure delivery of its security obligations". This change would more accurately reflect the policy intent and would allow suppliers to make the best use of the resources available.

- Z14: The audit must be undertaken by a Competent Independent Organisation, however there is

no requirement that the individuals performing the actual audits are competent to the appropriate level, just that the organisation is. We believe that in order to ensure that all parties achieve the same level of confidence in the audit process that the audit must be carried out by individuals within the organisation who hold relevant qualifications.

- Z14.b: It is unclear if the intention is for the audit to be carried out in the next calendar year, or within the 12 months immediately following the original audit. I.e. if the first audit is carried out in Jan 1st 2013, does the next audit need to be carried out on or before Jan 1st 2014 (12 months after the original audit), or by the end of 2014 (in the subsequent year). We believe that the intent is that the audit should be carried out 12 months after the previous audit and we support this approach. As such we believe that the condition should be reworded to provide greater clarity. We believe that the wording should be changed to: "at intervals of no greater than 12 months thereafter".

- Z17: Whilst we agree that there needs to be a way to ensure that programme is able to respond to new security challenges and threats; and we agree that there should be a mechanism to ensure that all suppliers are meeting a common baseline; we do not believe that the Secretary of State should hold these powers. Instead the Authority should solely hold the ability to apply these directions as they have the responsibility to enforce all licence conditions and this would be inline with existing practice.

- Z17.a: conditions (i) and (ii) are superfluous as they are covered by (iii) through (vi) and as such should be removed. In addition we feel that (i) may be used to direct suppliers to undertake additional trials into security related aspects of the programme which would lead to additional costs and potentially a higher number of stranded assets, which is not in the policy intent.

- Z17.a: The wording of the first sentence should be changed from "take (or refrain from taking) such steps" to "take (or refrain from taking) such **reasonable** steps". This will ensure that the directions are not used for unwarranted purposes, and it will also ensure that there is the ability for suppliers to challenge directions that are not reasonable and not in the best interests of the programme and the consumers.

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 would expect to perform these tasks as part of our day to day operations. This would include risk assessments, good security practice and managing security in our supply chain. We agree that these disciplines and procedures should be common across the whole of the Smart programme.

We agree that ISO27001 is the most appropriate standard to use as a systematic basis for managing the security of the Supplier End to End System as it covers all of the main security areas and is internationally known.

The foundation period is a learning period for all parties involved (suppliers, manufacturers, installers,

the Authority etc). As such it is anticipated that suppliers may improve their security approach and arrangements as they gain experience during the foundation period. The licence conditions should recognise the benefits of continuous improvement inherent in the ISO27001 standard.

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.

We believe that security is one of the costs of operating in the Smart market and should apply to all parties involved in the industry regardless of the size of the organisation or the size of the roll out plan.

As customers have the ability to move between suppliers, each supplier needs to have the confidence that the meters and communications services inherited through gained customers are secure. We would not want to see a situation where suppliers revert acquired meters to dumb/traditional because there is no confidence that the original supplier has met all of the security obligations.

As the licence only covers the period up until the DCC goes live, there is currently no visibility of the licence conditions that will apply to Smart meters that are not enrolled in the DCC once the DCC goes live. We expect that security of the non-DCC meters and transitional security will be covered fully in the proposed enduring security consultation.