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

27 July 2012

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

EDF Energy is one of the UK's largest energy companies with activities throughout the energy chain. Our interests include nuclear, coal and gas-fired electricity generation, renewables, and energy supply to end users. We have over five million electricity and gas customer accounts in the UK, including residential and business users.

EDF Energy welcomes the opportunity to respond to the Government's consultation on the proposed licence conditions for security risk assessments and audits in the period prior to the DCC providing services to smart meters. We believe it is essential for all licensed suppliers and any third party service providers with access to data from smart meters or smart meter functionality, to have undertaken appropriate and consistent security risk assessments for any smart or advanced meter systems installed prior to the DCC go-live date. Protecting our customer's personal and private information is one of our top priorities.

The ISO27001 Information Security Management System (ISMS) standard is a recognised risk management process for businesses. The ISMS process allows a business to understand its assets, the value of these assets, the threats and vulnerabilities to the assets and apply appropriate cost effective controls to protect them. EDF Energy agrees that the use of ISO27001, as a standard for managing security risks, is appropriate for all parties, that are operating within the smart metering system and/or have access to smart metering data, information or provide relevant supplying devices.

The implementation of an ISO 27001 framework for smart metering systems before the DCC is operational is a positive step towards gaining appropriate management of data when mass roll-out of smart meters occurs in the enduring environment commences.

However, we do not believe that the draft licence conditions deliver the policy intention outlined in the consultation document. The licence condition as drafted wavers between the requirement to be "secure" or to have a risk managed framework. These are completely different requirements.

Although it is our aspiration to protect all information, it is neither possible, nor cost effective, to be fully secure. We believe that the proposed licence condition should be re-drafted in line with the policy intent of the consultation to allow suppliers to implement appropriate, cost effective, security controls within the ISO27001 framework to protect customer information and the service as a whole.

EDF Energy
40 Grosvenor Place, Victoria
London SW1X 7EN
Tel +44 (0) 020 7752 2187

edfenergy.com
sustainability partner

We believe that for the whole industry should work from a set standard. DECC should ensure all suppliers are aligned by producing a:

- Standardised, ISO27001 scope.
- Industry wide risk appetite statement to ensure consistent controls are applied.

This is essential to ensure a consistent approach is adopted across the industry. Otherwise when a customer changes supplier the security risks and controls of the existing smart meter installation may not be aligned and there is a high probability of the meter installation not being trusted by the incoming supplier. This would result in the current meter either being adopted as dumb or replaced by the incoming supplier and therefore the meter assets becoming stranded.

There must be a clear distinction between this proposed licence condition and existing legislation such as the Data Protection Act (DPA). We believe that the proposed licence condition must not conflict with the DPA or replicate obligations already covered by the existing statutory framework.

Our detailed responses are set out in the attachment to this letter. Should you wish to discuss any of the issues raised in our response or have any queries, please contact my colleague Ashley Pocock on 01293 898595, or myself.

I confirm that this letter and its attachment may be published on DECC's website.

Yours faithfully

Attachment

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

EDF Energy's response to your questions

Consultation Questions

Q1. 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.

Annex A - Z1
The use of the term "Smart Metering Systems installed at premises" implies that these conditions are only applicable once the meter is installed. However, we believe it should cover the lifecycle of the components of a metering system that is either installed or which has previously been installed including, for example, during the disposal process. In addition, we believe the wording of the licence condition could be improved further to provide additional clarity on circumstances where a 'smart metering system' is operated in 'dumb' mode following a change of supplier. We believe these provisions should not apply to such circumstances.

Annex A - Z1
The use of term "maintain a high level of security in accordance with good industry practice" should be re-drafted to be more specific as the use of "high" is not a defined term within the proposed licence condition and neither is "good industry practice".

Annex A - Z2-Z3
The licence condition contradicts the consultation document. Is this proposed Licence condition valid up to DCC go live or SEC go Live?

Annex A - Z5
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. The categories should be aligned.

Annex A - Z6
EDF Energy believes that the requirement that "results in any other unauthorised access to data", "or causes any loss, theft or corruption of data" should state "all reasonable steps" to protect data from unauthorised access or loss in line with the policy intent of the consultation to allow suppliers to implement appropriate, cost effective, security controls within the ISO27001 framework to protect customer information.

Annex A - Z8
EDF Energy proposes that it is sensible to remove the square brackets from "[take all reasonable steps to ensure that it is able to comply]" from the proposed licence condition.

Annex A - Z10(c)
The use of "any" should not be used here, or there should be a clear definition of what a "security incident" is.

Annex A - Z12
EDF Energy proposes that "appropriate members" is changed to "designated members".

Annex AZ - 14
Where there is an initial audit requirement within the first six months EDF Energy would like to understand the scope of this initial audit and what DECC are expecting i.e. if this is to demonstrate full compliance or show road/Programme map to compliance.

Annex A - Z16a
EDF Energy proposes that "appropriate members" is changed to "designated members".

Annex A - Z16b
To allow for records to be kept in electronic form and to help with our green agenda, we propose that records using electronic media or other archive solutions/tools can be used.

Annex A - Z17
The use of "any" & "potential" are loose terms. While EDF Energy supports the ability for the Authority to issue Directions to take (or refrain from taking) steps as may be set out in any such Direction, we are concerned on whose advice and any industry consultations would this be undertaken. EDF Energy believes that this central body should be formed from the energy suppliers, UK Technical Authority (CESG), CPNI, Ofgem, Energy UK and DECC for such purposes.

Annex A - Z20
To fall within the definition of a "Competent Independent Organisation (CIO)" asks for a company that employs various CLAS and CHECK consultants. However, such consultants may not be suitably qualified in ISO27001 verification. We believe any assessments of the approach to, or audits of, the ISO27001 process should be conducted by suitably qualified and trained ISO27001 Lead auditors. The use of staff with CLAS/CHECK/CPA credentials but not ISO27001 trained and qualified should not be used.

Q2. 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?

EDF Energy believes that ISO27001 with the correct scope and alignment throughout the industry is an appropriate standard to follow to ensure a consistent assessment process of security risks.

There needs to be a standardised ISO27001 scope and industry wide risk appetite for the programme. This needs to be defined by DECC to ensure all suppliers and third parties who may access customer data, are aligned.

As mentioned earlier, where there is an initial audit requirement within the first six months EDF Energy would like to understand the scope of this initial audit and what DECC are

expecting to see i.e. if this is to demonstrate full compliance or show road/Programme map to compliance.

As mentioned previously any assessments of the approach to, or audits of, the ISO27001 process should be conducted by suitably qualified and trained ISO27001 Lead auditors. The use of staff with CLAS/CHECK/CPA credentials but not ISO27001 trained and qualified should not be used.

Q3. 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.

The scope and the assessment process needs to be consistent across all licensed suppliers no matter how small or large or how many meters are being deployed in this stage of the process. Any security breach even by a small supplier could bring the whole Smart Meter Programme into disrepute buy damaging customer trust.

EDF Energy
July 2012