e·on

Response to Consultation Security Risk Assessments

General Comments

We broadly agree with the approach. These are sensible steps in line with good practice.

Delivering end to end security is an important step in minimising asset stranding, maximising interoperability and delivering public confidence in Foundation. In order for suppliers to have confidence in the proposed framework, it is important that all suppliers start their risk assessments from a comprehensive and sustained baseline / common view i.e. the Security Technical Expert Group (STEG) risk assessment.

Our assumption is that these conditions will be applied to all suppliers. We are concerned that by not doing so, the programme would introduce unnecessary and unacceptable risk, as well as distorting the market.

We agree that all suppliers who are active in the Foundation period should carry out a risk assessment and that this should lead to development of an Information Security Management System (ISMS). We also agree that suppliers should seek to align their ISMS with the ISO27k standard suite. We believe that this alignment should be demonstrated by providing evidence of progress towards attaining formal certification, which represents minimal, if any, additional complexity, effort or cost beyond that implicit in the draft licence condition.

We understand that government is concerned that mandating a commercial standard such as ISO27001 may be open to challenge but are not aware of any equivalent standard that will meet the implicit requirements of the G.B. smart metering programme for that standard to be authoritative, proven, unambiguous and publicly recognised. We therefore suggest that government quickly undertakes a very short study, similar to that carried out to establish a standard for the Home Area Network (HAN), to reach agreement on which single standard is best suited for the purposes of smart metering security and privacy in G.B.

We are concerned by the process under which the Secretary of State (SoS) or the Authority may from time to time issue directional notices to suppliers. There is no indication either in the consultation or the draft licence conditions as to what process is to be undertaken to arrive at such a decision or what notice period(s) will be placed on suppliers within which they should conform to any such decisions.

We are surprised that the licence condition appears to be limited to the Foundation period only. We had expected that these conditions would continue to apply to all meters installed that remain outside of the jurisdiction of the Data Communications Company (DCC). It is not clear to us what the benefit of time limiting this condition provides.

e·on

Responses to specific 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.

We are generally comfortable with the licence conditions. We have the following specific comments;

We have concerns over the use of general phrases such as "high level of security" which is open to a wide interpretation together with use of absolute terms such as those used in clauses Z.6 & Z.17. For example terms such as "not subject to" and "any" are rarely if ever achievable in terms of cyber security. It may therefore be more appropriate to establish the intent of such clauses through an obligation to "maintain a level of residual security proportionate to the identified risks, whilst ensuring that the security requirements within Smart Metering Implementation Programme (SMIP) are implemented".

We are supportive of the intent of clauses Z.9 to Z.13 but believe these may represent a selective inclusion of a sub set of requirements and controls, all of which would be represented in any standard selected on the basis of meeting the intention of clause Z.8.

We agree that all suppliers who are active in the Foundation period should carry out a risk assessment and that this should lead to development of an Information Security Management System (ISMS). We also agree that suppliers should seek to align their ISMS with the ISO27k standard suite. We believe that this alignment should be demonstrated by providing evidence of progress towards attaining formal certification, which represents minimal, if any, additional complexity, effort or cost beyond that implicit in the draft licence condition.

We understand that government is concerned that mandating a commercial standard such as ISO27001 may be open to challenge but are not aware of any equivalent standard that will meet the implicit requirements of the G.B. smart metering programme for that standard to be authoritative, proven, unambiguous and publicly recognised. We therefore suggest that government quickly undertakes a very short study, similar to that carried out to establish a standard for the Home Area Network (HAN), to reach agreement on which single standard is best suited for the purposes of smart metering security and privacy in G.B.

In order to achieve independent audit 3rd Party Assurance, we do not consider that proposals to include CLAS, CHECK and CTAS organisations, accredited as they are by CESG for government purposes, to be appropriate. These organisations in our view do not meet the Competent Independent Organisation (CIO) criteria and they may not reliably and

consistently have the necessary skills and experience sought by the intent of the proposed conditions.

We therefore consider that an appointed CIO auditor should meet additional criteria of being commercially meaningful and publicly recognised as such by an independent body (namely UKAS) as meeting a definitive standard. In this context therefore, the obvious parties available are the ISO27001 Certification Auditors which further underscores the pragmatism of ISO27001 certification.

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?

We fully support the approach combining self assessment, a definitive standard and 3rd party assurance via audits.

Given the evolving nature of smart metering services during the Foundation period coupled with the probable material changes to cyber security threats during the same period, we consider that an annual audit regime is a sensible minimum. Adoption of the ISO27001 certification brings with it a 6 monthly auditing cycle, found tolerable in most sectors.

Delivering end to end security is an important step in minimising asset stranding, maximising interoperability and delivering public confidence in Foundation. In order for suppliers to have confidence in the proposed framework, it is important that all suppliers start their risk assessments from a comprehensive and sustained baseline / common view i.e. the Security Technical Expert Group (STEG) risk assessment.

Without this common view of risk it is likely that suppliers will take different approaches, and potentially place different obligations upon their supply chain(s) which will bring additional challenges at change of supplier events and intolerable risk exposures in operation. For example, when suppliers gain customers with assets operated and installed by different parties, it will not be possible to understand what has or has not taken place to assure the product in situ and to what standard any such assurance has taken place. This will result in additional protections (firewalls etc) being installed inconsistently by suppliers, adding unnecessary costs and ineffective security.

e·on

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.

Our assumption is that these conditions will be applied to all suppliers. We are concerned that by not doing so, the programme would introduce unnecessary and unacceptable risk, as well as distorting the market.

It would be unfortunate if government considered that exceptions or derogation of conformity could be applied to certain parties. We are firmly of the view that security is an area where government and or Ofgem cannot relax its requirements, where the goal must be to deliver true, overall assurance of end to end security. To not do so will introduce unnecessary risks and the reputation of the programme may then be called into question and potentially irreparably damaged.

We firmly believe that all suppliers should seek to align their ISMS with the ISO27001 standard. We believe that this alignment should be demonstrated by providing evidence of progress towards attaining formal certification, which represents minimal, if any, additional complexity, effort or cost beyond that implicit in the draft licence condition.

We are concerned by the process under which the Secretary of State (SoS) or the Authority may from time to time issue directional notices to suppliers. There is no indication either in the consultation or the draft licence conditions as to what process is to be undertaken to arrive at such a decision or what notice period(s) will be placed on suppliers within which they should conform to any such decisions.

It would seem appropriate that the SoS or Authority would in fact have to consult and take advice from internal and potentially external organisations in order to fully understand the risks and implications arising from such a decision. We believe that a suitable Security Management body will be needed and from the start of the licence condition's validity rather than from the advent of the Enduring environment. We suggest that this could be a revitalised STEG.

We are surprised that the licence condition appears to be limited to the Foundation period only. We had expected that these conditions would continue to apply to all meters installed that remain outside of the jurisdiction of the Data Communications Company (DCC). It is not clear to us what the benefit of time limiting this condition provides.