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

Email to: smartmetering@decc.gsi.gov.uk

Ref: URN 12D/234

SSE
REDACTED
REDACTED REDACTED REDACTED
REDACTED
REDACTED REDACTED

19 October 2012
REDACTED
REDACTED

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

SSE is pleased to provide comment on the draft licence conditions relating to security risk assessments and audits in the period before DCC provides services to smart meters. We welcome the ongoing engagement with the Smart Metering Implementation Team and have provided answers to the specific questions posed by DECC in the attached annex. We have also included specific comments on the proposed licence drafting

Please call me if you have any questions

Yours sincerely

REDACTED

Regulation

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.**

Overall, SSE agrees that the draft licence conditions lay the foundations to deliver the appropriate security requirements required for the Foundation period of the programme. SSE considers it appropriate and necessary for us to have undertaken appropriate security risk assessments for any smart meter installed prior to the DCC go-live date. However, SSE would like to see more detail in relation to suppliers having to accept the end to end risk when certain smart meters' security maybe supplied and controlled by other suppliers/parties.

SSE would also like to seek a better definition to section Z4, due to the complexities and ever changing environment no system can be deemed 100% 'secure'. SSE would prefer the definition to reflect the proposed ISO standards and ensuring appropriate controls in place.

We also believe the drafting of licence condition Z4 should include 'reasonable' in relation to taking such steps that the Supplier End-to-End System is secure at all times. Without this, SSE is concerned that a supplier can be held accountable for any circumstance that results in a failure of the security of the system even although this is outside the control of that supplier.

For example, one circumstance that is outside of the suppliers control would be if a customer was to be subject to theft (as the licence condition poses responsibility of the ancillary devices with the supplier). Whilst SSE appreciates the likelihood of this is remote, if the supplier is responsible for the hardware at the premises this would appear to particularly onerous as the licence condition as drafted at Z5 does not take into account physical act of data theft or consumer behaviour etc.

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?**

SSE is supportive of the approach proposed and at this current time ISO 27001 appears to be the most relevant minimum standard to which suppliers should achieve. SSE would hope that all suppliers would recognise this as a minimum standard and, through specific risk assessments, strive to increase security standards in critical areas.

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.**

SSE welcomes the requirements to work to industry standards and values the consistency that this could bring amongst suppliers. However, the requirement for 'good industry practice' needs to be firmer to avoid ambiguities, this should include a unified security architecture and standards relating to common security technologies.

SSE feel that from a Security and Risk prospective there would be great benefit of a phased approach to meeting these licence requirements. Once implemented, following these licence conditions all suppliers will have to make significant investment in security technologies that may well have to be replaced once the full security architecture of SMETSv2 is fully understood. A good example of this is Key Management (Encryption), currently there is not enough detailed requirements to understand what suppliers will have to have in place for SMETSv2. A phased approach would allow suppliers to provide tactical solutions in accordance to the size of there roll out of SMETSv1 meters enabling suppliers to concentrate their resources on working towards SMETSv2 and the introduction of the DCC.

We would also value that somehow suppliers have the ability to share Best Practise or ambiguities of the standard in an appropriate and timely manner.

Other Comments:-

Z.7 (b) This condition should be left to a reasonable time frame. A supplier should not be expected to produce evidence to the Authority upon request.

Z13. This should be left to the sole discretion of the supplier to ensure compliance and should not be included specifically in the Licence.

Z13. SSE must only be required to use reasonable endeavours to establish all appropriate physical and environmental security controls in accordance with good industry practice. It would be impossible to maintain all physical and environmental controls as no process is 100% secure, regardless the efforts a supplier makes.

Z15(b) - should be subject to reasonableness. SSE should only be required to undertake reasonable recommendations of the auditors. SSE could be requested to undertake an action that is wholly disproportionate to the costs of the action.

Z16 - should this not be left to our own discretion?