



ESP Utilities Group
Hazeldean
Station Road
Leatherhead
Surrey
KT22 7AA

T
F
Info@espipelines.com
www.esputilities.com

Mr. Tim Wates

By email only to
smartmetering@decc.gsi.gov.uk

29 November 2013

Dear Mr. Wates,

Response to SEC (Stage 2) consultation

I am writing on behalf of ES Pipelines Ltd, ESP Connections Ltd, ESP Networks Ltd, ESP Pipelines Ltd and ESP Electricity Ltd (collectively 'ESP'), in response to your '*A Consultation on New Smart Energy Code Content (Stage 2)*' document, published 17 October 2013.

Please see ESP's short response to specific questions relating to security in the annex below.

We appreciate the opportunity to respond and I welcome any questions or queries you may have in relation to ESP's response.

Yours sincerely,

ESP Utilities Group Ltd

ANNEX

Security

Q17 Do you have any comments on the security obligations set out in Section G of the SEC drafting or the way they are expressed?

Clause G3.1b (duty to keep register of hardware/software)

ESP we see keeping a list of software, including firmware versions/patches installed extremely challenging. For example, in relation to operating systems – keeping a list of service packs up to date is possible, whereas recording individual updates to every system on ESP's network is unfeasible given the volumes.

Can this clause be clarified so that the level of detail required is clear, or tied in to a party's ISMS, leaving it for each party to determine the risk posed by certain system updates and thus the level of detail required in the hardware/software register.

Clause G3.7b (duty to hold an audit by an external party prior to material system changes)

If the intention of carrying out an external audit prior to implementation of material system changes is to capture any new vulnerabilities arising from the change, does this need to be more explicit in the obligation? Or will auditors/parties be expected to take into account future changes when carrying out an audit prior to system changes?

How is the materiality of a change to be assessed - materiality in relation to cost, potential threat to systems, scope of change?

Q18 Do you have any comments on the appropriateness and / or the proportionality of the security obligations in relation to particular types of DCC Service Users and their role?

Clause G3.7a (duty to hold an audit by an external party annually)

Where a party holds the ISO27001 accreditation across its entire company and consequently has an annual audit carried out in relation to that standard, is it envisaged that the ISO27001 audit satisfies this requirement or are parties expected to hold a separate audit? Is it possible for this to be clarified in the drafting?