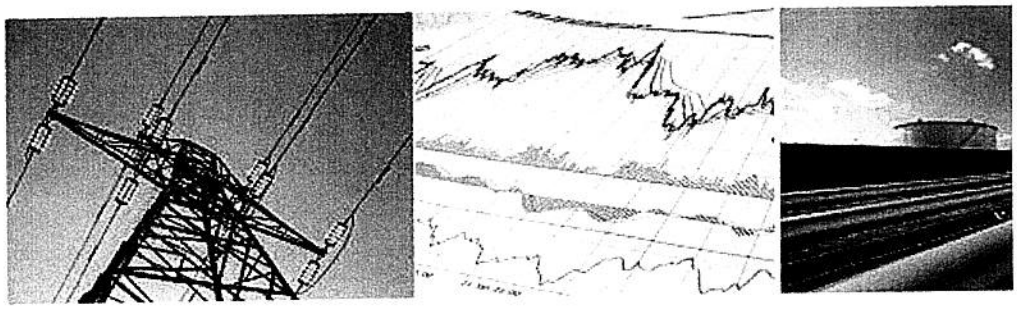
Department of Energy & Climate Change (DECC)
Smart Metering Implementation Programme



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

from HP Enterprise Services UK Limited

27th July 2012

Table of Contents

Copyright and Usage

Background - HP

Hewlett-Packard is a technology solutions provider to consumers, businesses and institutions globally. Our offerings span information technology (IT) infrastructure, personal computing and access devices, global services, and imaging and printing.

Hewlett-Packard counts nearly all of the global Fortune100 companies as customers and is proud to serve as the preferred vendor of IT products and services to thousands of large enterprise customers worldwide. The fact that these companies entrust HP to power their critical business operations is testimony to HP's strength as a proven, reliable supplier of enterprise solutions.

In 2008 HP acquired Electronic Data Systems Corporation (EDS) and formed HP Enterprise Services. HP Enterprise Services provides infrastructure technology outsourcing services, applications services, and industry services, including business process outsourcing. HP now provides one of the broadest portfolios of products, services and end-to-end solutions in the technology industry. The combined offerings are focused on helping clients accelerate growth, mitigate risks and lower costs.

HP Enterprise Services leverages the breadth of the HP portfolio and our Best Shore® delivery strategy to offer comprehensive IT services to more than 1,000 business and government clients in 90 countries. We have a wide range of clients in the UK and Ireland in the following industries:

- Financial Services
- Healthcare
- Local and Central Government
- Manufacturing
- Retail
- Telecoms/Network Service Providers
- Public Sector

Introduction

HP welcomes the opportunity to respond to the DECC's consultation on pre-DCC security management, issued on 31st May 2012. We believe that the introduction of smart metering will benefit consumers, suppliers, UK plc and the environment, supporting the transition to a low-carbon economy and helping to provide affordable, secure and sustainable energy.

We have based our response to the consultation on our experience as a leading provider of IT and related services; our 30 years of global experience in the utilities industry; and our understanding as a leading IT supplier to the UK government. We have extensive experience in helping public and private sector organisations improve their operations through advanced technology and business process improvement, in areas which include energy management, privacy, security, safety, customer focus and data transfer services.

We are supporting smart metering programmes for utility clients around the world; have developed deep understanding of the importance of advanced metering infrastructures (AMI) to support the introduction of Smart Grids; and have introduced a Smart Meter Managed Service (SMMS) offering.

As a company, we are a recognised leader in sustainability, providing IT services and solutions - to government and business clients as well as domestic consumers - that improve energy and cost efficiencies, reduce carbon emissions, conserve natural resources and achieve competitive advantage.

Our responses to the consultation in general, and to some of the specific questions raised by DECC, follow.

Response to Consultation

General Comments on the Consultation Document

The purpose of the consultation is to request views on a draft licence condition relating to security risk assessments and audits in the period before the Data and Communications Company (DCC) provides services to smart meters. This period is in general called the Foundation stage and the service provided by the DCC represents the Enduring stage.

Clarity is needed to define what the "date of SEC Go Live", means in practice.

The DCC will take on all Foundation stage meters at a defined date. In practice there is an Industry expectation that there will be a ramp up of pre SMETS and SMETS 1 meters from Foundation stage Smart Meter System Operators (SMSO) into the DCC User service. This will mean that both Foundation and Enduring stage meters will be providing services to Consumers in parallel for potentially an extend period of time.

As a result, the certification against ISO27001 (for the end to end Foundation stage) continues past the date when the DCC goes live and this may be for some years past "SEC Go Live".

HP Responses to Specific Questions

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.

Response:

Yes the draft license conditions deliver the policy intention. The drafting can be improved by incorporating the following suggested amendments and clarifications:-

- Clear and agreed definition of "SEC Go Live" date or provision for an extended period of time relating to the drafting.

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?

Response:

HP has provided a summary document that considers the potential impact of this proposed approach on the Smart Meter Managed Service; "*SMMS Foundation Stage Security Risk Assessment, Consultation on a draft licence condition relating to security risk assessments and audits prior to DCC service provision v1 dated 25 July 2012*".

The activities that are recommended over the next period of time (approximately 24 months) to achieve a Foundation end to end solution that includes ISO27001 certification as a goal have been discussed. The roles of each industry stakeholder in the certification process has been identified (using a RACI approach), and the practical steps needed to establish Information Security Management System (ISMS) documentation and work-packages defined.

In the general case it is proposed that the following actions are undertaken over the next period of 6 months:-

- A competent security organisation is requested to quote for an initial risk assessment of the end-to-end system. This will need cooperation and commitment from the identified RACI contributors to the systems as a whole. The method proposed will use the capabilities required of a Competent Independent Organisation (e.g., CLAS and CHECK). It is unclear, at present how the Authority and stakeholders will fund this work.
- A Security Working Group (SWG) is formed by the stakeholder organisations to establish governance for this process and establish the Appropriate Standard for each of the RACI service providers. This may be an extension to the role of the STEG.
- The SWG determines the initial ISO27001 Gap Analysis between existing ISO certifications and Authority defined end-to-end "Appropriate Standard" for each stakeholder organisation. This will ensure compliance with the Authorities specific standards, policies and applicable regulations especially where it relates to "Change of Supplier".
- Each stakeholder organisation reports to the SWG an estimate of the business cost, investment and deployment plan to close the identified Gaps. The SWG should then create and publish a plan for implementation and ISO27001 certification for the end-to-end system.
- Each stakeholder organisation should then obtain business approvals to proceed and execute the business plan over an 18 month window.

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.

Response:

The attached whitepaper outlines a proposed general approach by suppliers. An estimate of cost for the whole end to end process is difficult to establish. This is because the amount of practical effort and the costs of certification or audit by a Competent Independent Organisation are dependent upon the gap analysis and amount of work associated with work-packages.

However, an initial estimate for the first work-package "An initial risk assessment of the end-to-end system" is

- 70 man days of effort using CLAS or similar resources
- with support from the 6 RACI stakeholders.
- Input from each stakeholder will be needed and this is estimated at 5 man days per stakeholder (30 days).
- This initial work-package (of up to100 days), would be tasked with identifying the costs of further work-packages.

The impact of "Change of Supplier" needs to be considered. Should there be some form of waiver associated with a supplier that is unable (due to is size), or is not able to subscribe to a ISO27001 certification plan? What happens if the new supplier is not based within the UK and needs to establish a process of certification outside for example the BSI? There is the possibility that some Industry participants may leave an "ISO27001 certification gap" when consumers move between Energy Suppliers. An approach to extending the role of the STEG may enable resolution and management of such cases.