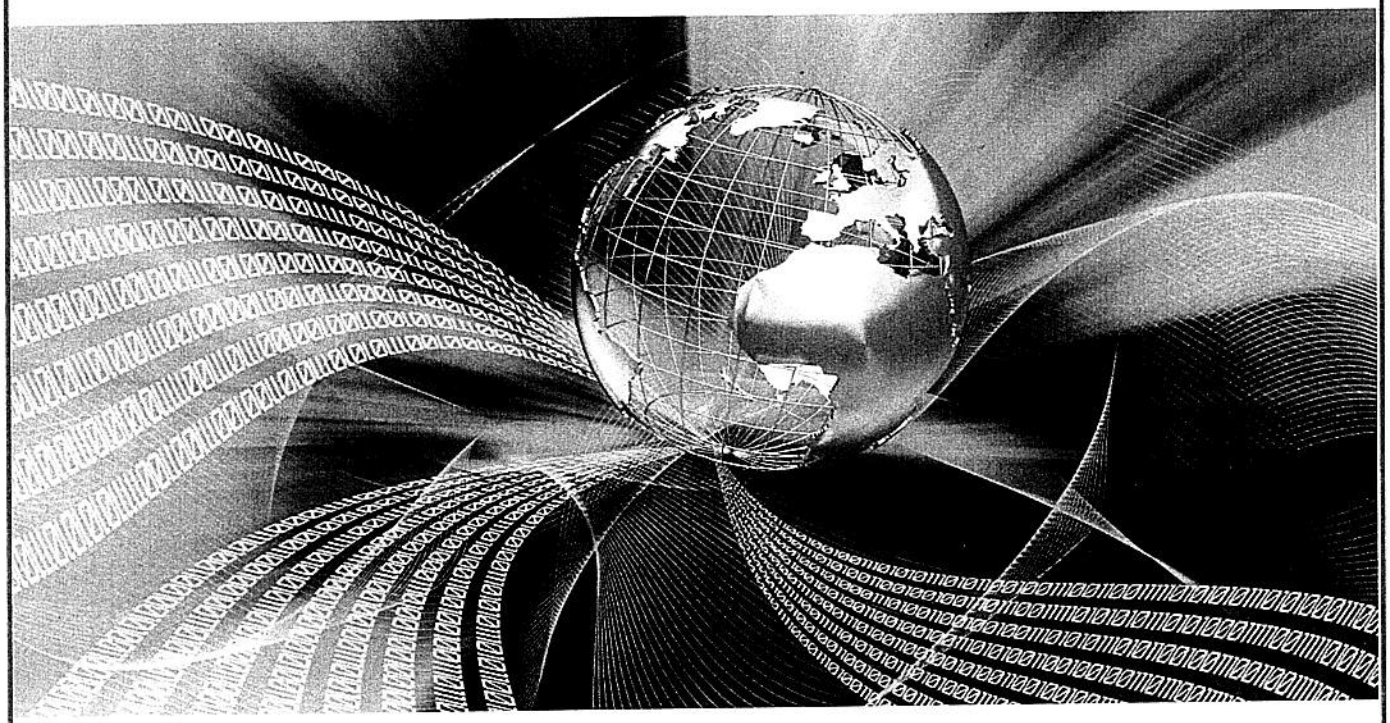
Smart Metering Implementation Programme



Response to

Department of Energy & Climate Change

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

Amethyst
Risk Management Limited
Leadership in thought & action

Document History

Our Reference:	726-01
Version:	1.0
Date:	27 July 2012
Author:	
Reviewer:	
Quality Assurance:	
Your Reference:	URN 12D/234

References:

[A]	DECC Consultation reference URN 12D/234 – Smart Metering Implementation Programme – Request for comments on a draft license condition relating to security risk assessments and audits in the period before the DCC provides services to smart meters. Issued 31 May2012
[B]	HMG IA Standard Numbers 1 & 2 – Supplement – Technical Risk Assessment and Risk Treatment Issue No.1.0 April 2012
[C]	CESG Technical Threat Briefing – Assessment of Technical Threat Issue No. 1.0 September 2011
[D]	CESG Supplier Information Assurance Assessment Framework and Guidance Issue No.1.0 January 2011
[E]	HMG IA Standard Numbers 1&2 Information Risk Management Issue No.4.0 April 2012

Worting House, Church Lane, Basingstoke, Hampshire, RG23 8PX

Tel

www.amethystrisk.com

Contents

1 Introduction

1.1 In its consultation paper [A] the Department of Energy and Climate Change (DECC) seeks comments on a draft license condition relating to security risk assessments and audits in the period before the Data and Communications Company (DCC) provides services to smart meters.

1.2 In preparing this response, Amethyst Risk Management Ltd. (Amethyst) has consulted with its partner company, Secada Ltd. (www.secada.co.uk).

1.3 The consultation paper asks for responses to three specific questions:

a. 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.

b. 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?

c. 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.

1.4 Please see Section 2 for our response to each of these questions.

2 Response to Questions

Response to Question 1

2.1 The draft licence conditions will not deliver the policy intention as outlined in the consultation document. There are a number of reasons for this assertion, but it is appropriate to consider some related questions, possible omissions, and alternative approaches.

Response to Question 2

2.2 We have a number of comments on the proposed approach that suppliers should carry out a number of good practice security disciplines and procedures.

Response to Question 3

2.3 We have a number of general comments and observations around the approach to small suppliers, the processes expected of suppliers in general, and any related costs.

Smart Metering & CNI

2.4 Although the consultation document infers that the end-to-end system may be regarded as part of the Critical National Infrastructure (CNI) e.g. paragraph 1.2 states "...the Programme already works with energy suppliers and experts from relevant government agencies..." there is no explicit statement to this effect. Given that the draft licence conditions have a focus on industry best practice for security i.e. ISO 27001 rather than any specific government standards, it might equally be assumed that the end-to-end system is not part of the CNI. Our assumption, for the purposes of this response, is the latter i.e. that the end-to-end system is not part of the CNI and therefore industry best practice for security is an appropriate response.

2.5 We also believe there is a distinction to be drawn between smart metering for domestic customers versus industrial/commercial users. It seems probable that for the former, discreet personal information will be present, as suppliers wish to design tariffs based upon usage. Such data is likely to be sensitive on a number of levels e.g. it may clearly indicate dates/times when a particular property is empty. In the case of the latter, there may be smart metering of hospitals, Ministry of Defence sites, and Banks, some of which will undoubtedly be part of CNI. Risks associated with smart metering of these sites and facilities will therefore require a more rigorous assessment.

Smart Metering Business Impact Levels

2.6 In considering whether or not smart metering is part of the CNI, the question of Business Impact Levels (BIL) must be addressed. BIL are defined by CESG in the HMG IA Standard Numbers 1 & 2 – Supplement [B], Appendix B of which provides detailed examples of BIL as a basis for making judgments on the importance of any given data. If the end-to-end system is not part of the CNI and therefore industry best practice for security is an appropriate response, then BIL for the confidentiality, integrity and availability of smart metering are likely to be in the range of BIL 0-2. If such an assessment has not been made then our recommendation is that it should be, and in any event, the information is relevant

to and should be shared with the suppliers, perhaps in supplementary guidance rather than within the actual licence conditions.

Threat Information for Smart Metering

2.7 If suppliers are to perform valid risk assessments then they will need appropriate threat information, but neither the consultation document not the draft licence conditions make it clear where or how suppliers can gain access to it. This is an omission that should be corrected, whether by reference to generic threat information, or by arranging for supplier access to more detailed (and protectively marked RESTRICTED) threat information such as that provided by CESG [C]. Without valid threat information, the output from any risk assessment will be of little use. However, a more practical solution may be in the development of a single generic risk assessment for smart metering (see para 2.12).

2.8 Paragraph 3.9 of the consultation document incorrectly states that suppliers need to conduct ongoing risk assessments in order to identify changes to the **threat** environment. In fact historically the threat environment changes little over time, and in any case is not altered by conducting a risk assessment, the output from which will identify changes to the **risk** environment.

Proposed Approach

2.9 From a purely technical perspective the broad approach proposed in the draft licence conditions is basically sound, although reliance on standards per se is no guarantee of effective security. Equally, adopting an approach based solely on ISO 27001 naturally raises questions about other standards e.g. the ISO 28000 series on supply chain security, and ISO 22301 (replacing BS25999) on business continuity management, all of which are potentially valid in relation to smart metering systems and services. ISO 27001 is however a mature and widely recognised international standard and the requirement for independent audits of suppliers' compliance against this standard by Competent Independent Organisations (CIO) is a useful mechanism for providing assurance, and reflects an approach that we believe is being considered by other government departments. However, we would raise the following specific observations:

a. The draft licence condition (Part E. Z.20) defines what it calls an appropriate standard: "a high level of security that is in accordance with good industry practice and is capable of verification as such by a Competent Independent Organisation." Specifically, use of the term "high level" is not helpful as it is an entirely subjective one. In fact the need to specify an appropriate standard, beyond ISO27001, is questionable. It ought to be sufficient to require suppliers to demonstrate compliance with ISO 27001, stopping short of formal certification, with assurance of compliance provided by a CIO.

b. There already exists guidance and a framework for the assessment of supplier Information Assurance [D]. This takes a similar approach to that proposed by the draft licence conditions, based upon a set self-assessment questions that the supplier must answer. It incorporates a useful scoring mechanism and provides flexibility according to the specific business of the supplier. This might be an appropriate alternative rather than a one size fits all approach via ISO 27001, especially as it may be less costly and time consuming for smaller suppliers.

c. It is not clear whether the intention is for output from the proposed audits to be a simple pass or fail. If so, what criteria will the CIO rely upon in making the assessment and how will a consistent audit approach across all CIOs be achieved? It is conceivable

that DECC might need to develop and publish guidelines or metrics for CIOs as a means of ensuring that all suppliers are audited equitably.

2.10 In terms of the cost implications for suppliers of smart metering systems and services, the proposed approach will cause concern. Most if not all suppliers will lack the knowledge or expertise to implement ISO 27001 within their businesses and will therefore need to rely upon external consulting support. It is assumed they will also be expected to bear the cost of audit by a CIO. These costs will be ongoing, and are likely to be passed on to consumers.

How to Save Time and Reduce Cost

2.11 An overriding consideration in preparing the draft licence condition must be the time and cost implications for suppliers of smart metering systems and services. Time and costs for achieving ISO 27001 compliance vary according to a number of factors including the size and nature of the business, but are typically measured in months and tens of thousands of pounds. Even a simple feasibility study and gap analysis can cost a small business thousands of pounds.[1] The policy intention could therefore be described differently, but in terms that already exist and are widely applied both within government and by government suppliers, namely accreditation. HMG IA Standard Numbers 1&2 Information Risk Management [E] provides a description of accreditation that would seem to be applicable to the policy intention for smart metering, as follows:

> "The accreditation of ICT systems or services handling, storing or processing protectively marked information or business critical data is a formal, independent assessment against IA requirements, which results in the acceptance of residual risks in the context of business requirements and information risk appetite. Typically this will be a prerequisite for approval to operate."

2.12 The process of accreditation requires the development of evidence to support accreditation decisions. Such evidence must be proportionate and will typically include a technical risk assessment, IT Health Check (penetration test), and Security Operating Procedures (SyOPs). A number of government departments e.g. the Ministry of Defence and suppliers have developed fast-track processes for accreditation, some of which might be useful in the context of smart metering suppliers. The accreditation process should not be an onerous one, especially where systems and services are operating in the range of BIL0-2.

2.13 The proposed Competent Independent Organisations might operate on behalf of DECC to accredit end-to-end smart metering systems and services, and such an approach offers the possibility of a more efficient solution. For example, it is feasible that a generic risk assessment for smart metering could be developed, applicable to all suppliers of end-to-end smart metering systems and services. This could be developed by DECC and made available to the CIOs and suppliers, saving them time and reducing overall costs. Such an approach would be especially advantageous to smaller suppliers. Other core elements of accreditation evidence including SyOPs, risk registers, risk treatment plans and IT Health Checks could be 'shared' in a similar vein, the overall effect being one of greater efficiency, more rapid results, and lower costs.

Additional Comments & Observations

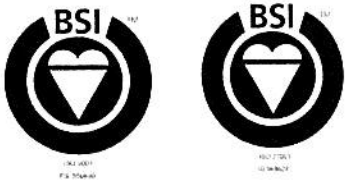
2.14 Additional comments and observations are at Annex A.

[1] As an example see http://www.itgovernance.co.uk/ISO27001-feasibility-and-gap-analysis-service.aspx indicating a cost of £5,900 for a single site SME with 501-2000 employees.

Annex A Additional Comments & Observations

Paragraph	Comment/Observation
1.1	Reference to 'privacy' is understood but 'confidentiality' may be more appropriate. Also, the consultation document gives no indication as to whether there is an expectation that smart metering systems will store or process personal information. Paragraphs 4.3.9.1 to 4.3.9.3 of the draft Smart Metering Technical Specifications April 2012 do however indicate the presence of personal data. The presence or otherwise of personal data within any smart metering system is of crucial importance and will have a significant bearing on the security measures that will need to be implemented. Where personal data is present, Privacy Impact Assessments (PIA) as recommended by the Information Commissioner may be required.
3.2	Consistency of approach will not be achieved unless the proposed CIOs perform audits to an agreed and common standard.
3.3	Suppliers have a duty to conduct 'ongoing risk assessments' but the draft licence conditions do not appear to specify this requirement. Any such requirement should also specify periodicity of risk assessments. This paragraph also states that the aim of such risk assessments is to 'identify new threats...' but risk assessments do not identify threats (see para 2.7 of this report).
3.12	Lists a number of disciplines expected of suppliers in addition to an ISMS, but the items listed are actually part of an ISMS.
3.13	States: 'Given the importance of maintaining secure smart metering systems...' This implies that such systems have a degree of criticality (see para 2.4 of this report in relation to CNI, and also para 2.5 on BIL). If these systems are critical, then they must be available, and availability is measured in terms of BIL. There is typically a close correlation between system availability, business continuity plans and service level agreements.
3.14 & Z.20	There is a disconnect between the schemes listed, which are all government schemes, and the core proposal which is based upon a commercial i.e. non-government standard (ISO 27001). It may therefore be more valid to specify that a CIO should have staff who are ISO 27001 lead auditors.
3.17	It is not clear who or what 'the Authority' is in this context.
3.18 & 3.19	These paragraphs and the related sections in the draft licence conditions (Z.17 to Z.19) confer considerable powers on the government and/or the Authority. Para 3.19 indicates that use of this power 'will not compromise consumer protection and the functioning of the market' but if the situation arises where one or more suppliers are required to act under the direction of the government or the Authority, then de facto the functioning of the market must surely be affected as a consequence. Any such powers of intervention and direction of suppliers can only be justified where the systems and services are sufficiently critical to the national interest; see previous comments and observations on the issue of criticality.

Paragraph	Comment/Observation
4.1	ISO 27001 and the ISMS are sufficiently flexible that the scope (via a statement of applicability) can be tailored to focus on say a particular aspect of a large or complex business, as well as to an SME.
5.1 – 5.3	Section 5 alludes to broader issues of governance to be the subject of future consultation. These will be critical to the effectiveness or otherwise of the proposed licence conditions. Para 5.3 refers to smart meters that are operated inside and outside of the DCC but does not explain the context.
Z.1	Should read: 'This condition requires the licensee to maintain an appropriate level of security commensurate with good industry practice...' This section includes 'associated software' within the scope of the condition. More clarity may be needed on this aspect, perhaps in supplementary notes rather than within the actual licence conditions, e.g. does this refer to all associated software including operating systems, applications and databases? Another question that might be anticipated is: to what if any extent will such software require independent assessment or evaluation of security functionality, and to what level?
Z.7 (b)	It is not explicitly specified who will decide and on what basis whether the subject documentary evidence is 'sufficient to demonstrate its compliance...'
Z.8	The term 'all reasonable steps' is highly subjective. An alternative wording is: 'The licensee must demonstrate compliance with...'
Z.10 (c)	An obligation should be placed upon suppliers to report details of all actual or suspected security incidents to government/the Authority. Effective incident reporting will allow for trends or patterns to be identified and provide an opportunity for risk reduction.



Amethyst Risk Management Limited
Worting House
Church Lane
Basingstoke
Hampshire
RG23 8PX
United Kingdom

Tel:
Fax:

sales@amethystrisk.com

www.amethystrisk.com

Amethyst
Risk Management Limited
Leadership in thought & action