DEPARTMENT OF ENERGY & CLIMATE CHANGE

Smart Metering Implementation Programme

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

31 May 2012

Department of Energy and Climate Change
3 Whitehall Place
London
SW1A 2AW

Telephone: 0300 068 4000
Website: www.decc.gov.uk

© Crown copyright 2012

Copyright in the typographical arrangement and design rests with the Crown.
This publication (excluding logos) may be re-used free of charge in any format or medium provided that it is re-used accurately and not used in a misleading context. The material must be acknowledged as crown copyright and the title of the publication specified.

This Consultation can also be found on DECC's website

Published by the Department of Energy and Climate Change.

Contents

General Information

Purpose of this consultation
To request views on a draft licence condition relating to security risk assessments and audits in the period before the DCC provides services to smart meters.

Issued: 31 May 2012

Respond by: 27 July 2012

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

Telephone: 0300 060 4000 Email: Matthew.Adams@decc.gsi.gov.uk

Consultation reference: URN 12D/234 – Smart Metering Implementation Programme – Request for comments on a draft licence condition relating to security risk assessments and audits in the period before the DCC provides services to smart meters

Territorial extent: This consultation applies to the gas and electricity markets in Great Britain. Responsibility for energy markets in Northern Ireland lies with the Northern Ireland Executive's Department of Enterprise, Trade and Investment.

How to respond: Your response will be most useful it is framed in direct response to the questions posed, though further comments and evidence are also welcome.

Responses to this consultation should be sent to smartmetering@decc.gsi.gov.uk no later than 27 July 2012.

Responses should be clearly marked "Request for comments on licence conditions relating to security risk assessments"

Hard copy responses should be sent to the address above.

Additional copies: You may make copies of this document without seeking permission. An electronic version can be found at: www.decc.gov.uk

Other versions of the document in Braille, large print or audio-cassette are available on request. This includes a Welsh version. Please contact us at the address above to request alternative versions.

Confidentiality and data protection: Information provided in response to this consultation, including personal information, may be subject to publication or disclosure in accordance with the access to information legislation (primarily the Freedom of Information Act 2000, the Data Protection Act 1998 and the Environmental Information Regulations 2004).

If you want information that you provide to be treated as confidential please say so clearly in writing when you send your response to the consultation. It would be helpful if you could explain to us why you regard the information you have provided as confidential. If we receive a request for disclosure of the information we will take full account of your explanation, but we cannot give an assurance that confidentiality can be maintained in all circumstances. An automatic confidentiality disclaimer generated by your IT system will not, of itself, be regarded by us as a confidentiality request.

We will summarise all responses and place this summary on our website at

http://www.decc.gov.uk/en/content/cms/consultations/cons_smip/cons_smip.aspx. This summary will include a list of names or organisations that responded but not people's personal names, addresses or other contact details.

Quality assurance: This consultation has been carried out in accordance with the Government's Code of Practice on consultation, which can be found here: http://www.bis.gov.uk/files/file47158.pdf
If you have any complaints about the consultation process (as opposed to comments about the issues which are the subject of the consultation) please address them to:

DECC Consultation Co-ordinator

3 Whitehall Place London SW1A 2AW

Email: consultation.coordinator@decc.gsi.gov.uk

Summary

In April 2012, the Government explained that it was minded to place a specific obligation on suppliers in relation to the security of their end-to-end smart metering systems[1], through a new licence condition. The intention was that this obligation would cover the period until the Data and Communications Company (DCC) starts to provide services, when there will need to be different arrangements in place. This condition would require suppliers to be responsible for the end-to-end security of their smart metering systems. In fulfilling this obligation, the Government stated that suppliers might also be required to conduct a risk assessment of their end-to-end systems and to have an annual security risk audit conducted by suitably qualified, independent, external specialists. This document presents and considers the specific licence obligations for these existing Government proposals for this early period (referred to here as the pre-DCC 'go live' phase). The Government will consult on the enduring arrangements in the coming months.

1. Introduction

1.1 The Government's objective is to ensure that the end-to-end smart metering systems that suppliers manage and operate, along with the equipment they install, enable a secure and reliable national infrastructure for energy supply, protecting consumers' interests and industry investment, and realising data privacy commitments. These are all key to securing consumer confidence in the system.

1.2 The Government is committed to ensuring security is embedded into the design process for smart meters and their communication systems from the start, and to create a framework that allows systems and processes to continue to be fit for purpose as security risks, technology, and the requirements continue to evolve. The Smart Meter Implementation Programme (the Programme) already works with energy suppliers and experts from relevant government agencies to help ensure there is proper preparedness for mitigating risks and taking appropriate actions to manage and operate secure systems. This process will continue. Given the potential for a security incident, of any nature, to undermine confidence in smart metering and hence impact the immediate and long term benefits associated with the Programme, the Government has proposed that obligations should be placed on suppliers in advance of DCC 'go live'.

2. Policy Approach

2.1 For security arrangements to be truly effective, they must be implemented in an end-to-end manner, across all parties and components that interact with the smart metering system. A failure or oversight of a security control in one element of the system could

[1] For the purposes of this document, the term 'end to end smart metering system' includes the smart metering equipment located within the consumer's premises, the communication network between the consumer's premises and the energy supplier, and the energy supplier's head end system, and all business procedures associated with the installation, operation and support of the system.

undermine the overall security solution. It is therefore crucial that as well as security being considered in the technical design phase, those responsible for security implement solutions in a proportionate and effective way across the full end-to-end system, including relevant business processes.

2.2 During the pre-DCC 'go live' phase, energy suppliers have more flexibility over the rate of deployment of smart meters. During this time, they will have end-to-end responsibility for the smart metering solution, including equipment which complies with the initial version of the Smart Metering Equipment Technical Specifications (SMETS). The initial version of SMETS sets out security requirements that equipment must support, including requirements relating to the encryption of data and authentication of the source of commands received. In later versions of SMETS it will be appropriate to specify the standards that equipment will need to be certified against as well as the certification procedures to be followed so that DCC can gain comfort that equipment that connects to it meets an appropriate level of security.

2.3 During the period when suppliers control all aspects of their end-to-end systems, they should implement their own security assurance regimes through their procurement, contract, and internal management processes. These regimes can be developed to ensure that equipment and communication systems will support the security requirements appropriate to their risk assessment and solution design, drawing on industry good practice.

2.4 All smart metering systems – including those that will be implemented before DCC 'go live' – need to address security threats to data privacy and confidentiality, and from unauthorised access to smart metering functions. To reflect and underpin the Government's expectations of suppliers' responsibilities for the security of their smart metering systems, the Government proposes to place specific obligations on suppliers in relation to the security of their end-to-end smart metering systems, through a new licence condition. This reflects the expected enduring arrangements, where the DCC, which will have overall responsibility for the security of the end to end smart metering system will have relevant conditions in its licence, imposing certain security-related obligations.

3. Implementing the Approach

Overview

3.1 As has been noted in previous publications, implementation of the Government's smart metering policy will require changes to the existing regulatory and commercial framework governing the electricity and gas markets. The Energy Act 2008 gave the Secretary of State powers to amend existing, or create new, licence conditions and industry codes for the purposes of delivering the Programme. Subject to responses received to this publication, and ongoing discussions with stakeholders, the Programme proposes to prepare a response to this document and a licence condition for Parliamentary scrutiny by the end of the year.

3.2 The draft licence condition proposed in this document requires certain activities to be undertaken by suppliers. It aims to achieve consistency of approach, and to provide reassurance that appropriate steps are being taken. The draft licence condition can be found at the end of this document and the individual steps are considered below.

3.3 As an overview, the licence condition provides an overarching duty on suppliers to ensure a secure system to an 'Appropriate Standard'. To do this, suppliers need to: conduct a risk assessment; design a solution for their end-to-end system to the desired level; conduct ongoing risk assessments to identify new threats taking into account the impact it could have on their systems; and implement mitigating measures. To complement this, suppliers would be required to have a security risk audit conducted by suitably qualified, external specialists. The audit would verify that: the risk assessment and solution design is in line with industry good practice and appropriate for the services provided; that the risk assessments had been properly determined; and that the mitigating measures selected are appropriate to treat the identified risks to the desired level.

3.4 The steps outlined in the draft licence condition are explained in more detail below. We welcome views on these steps and the way they are drafted in the licence condition. Noting that security incidents have the potential to bring costs to suppliers in terms of revenue loss, reputational impact and may have consequences to business continuity and smart meter rollout plans, we also welcome views on the costs and implications of the measures proposed here so as to complement the Programme's considerations.

Core elements of supplier licence conditions

Application (see sections Z.2 to Z.3 of the draft licence condition in annex A)

3.5 The licence condition has been drafted to capture the period until the DCC starts to provide services to SMETS meters. This is reflected in the draft licence condition through referring to the concept of the Smart Energy Code 'Go Live'.

Secure End-to-End Systems (Z.4 to Z.6)

3.6 Suppliers are required to take such steps and do such things as are within their powers to provide a secure end-to-end system. The end-to-end system includes the smart metering equipment located within the consumer's premises, the communications network between the consumer's premises and the energy supplier, and the energy supplier's head end system, and all the business procedures associated with the installation, operation and support of the system.

3.7 The licence condition states that the system is secure if it is operated to the Appropriate Standard. This standard is further defined in the licence condition as a high level of security that is in accordance with industry good practice and capable of being verified by a Competent Independent Organisation. Further information is provided about this below.

Supplier Information Security Policy: Risk Assessment, Risk Management and Risk Mitigation (Z.7 to Z.13)

3.8 The process of carrying out a comprehensive risk assessment is an important step in managing security risks. It requires an appreciation within the organisation of the level of risk that can be accepted and the potential impacts should an incident occur.

3.9 Requiring suppliers to conduct ongoing risk assessments is key to identifying whether there are changes to the threat environment. It is recognised that what is secure today may not always be secure, and an important element of a risk assessment is to have a thorough understanding of the threats to the smart metering systems. Equally critical to a risk assessment is to have an appropriate scope which allows risks to be identified in the first instance.

3.10 The risk assessment should drive a set of measures to mitigate identified risks in line with the Appropriate Standard it has set. This should be set in the context of an Information Security Management System (ISMS). This is a framework that enables organisations to continually design, implement and maintain their desired set of security policies, to leverage industry good practice, and provide a holistic security approach. To that end, the Government (through the licence condition) proposes that suppliers operating in the pre-DCC 'go live' phase should seek to align their security operations with ISO27001 during this period, although with no explicit requirement to become certified against this standard.

3.11 The Government recognises that not all suppliers would be in a position to certify themselves against this standard. For example, this might be because it is unnecessary for them to do so, or the demands of certifying against the standard are not proportionate to their rollout trajectory during the pre-DCC 'go live' phase. However, there is an expectation that suppliers will use this period to work towards attaining this standard and be able to demonstrate steps they are taking in this regard. The licence condition has been drafted to capture this intention, however we welcome views on this draft and whether this is a suitable approach.

3.12 In addition to a robust ISMS, there are a number of disciplines that the Government expects all suppliers to have in place, which include:

- A security policy, to govern the supplier's approach to risk assessment and treatment
- Incident management procedures, that enable suppliers to identify and respond to a security incident in a coordinated manner, minimising the impact to those that may be affected
- Business continuity and disaster recovery procedures
- Access to appropriately qualified security staff who can advise on matters related to security
- Physical security controls to protect equipment that interacts with the smart metering system.

3.13 While the Government recognises that the risk profile will differ between suppliers, given the importance of maintaining secure smart metering systems, the Government expects that suppliers will adhere to standards in line with good industry practice and that the standards adopted must be capable of being verified by a Competent Independent Organisation (CIO). The CIO is expected to assess whether the supplier's ISMS provides a level of protection in line with good industry practice that is also commensurate with the security risks.

3.14 The Government's proposal is that, a CIO is an organisation which has certain qualifications or characteristics such as being members of (or contain staff who are

members of) CESG[2] schemes, such as CCP[3], CLAS[4], CHECK[5] or CTAS[6], or a combination thereof. This is achieved in the licence condition by using the term "Appropriate Standard".

Independent Audit (Z.14 to Z.16)

3.15 To provide assurance that risks are being managed in line with the risk assessment and mitigation measures, the Government considers there is value in requiring suppliers to conduct an independent audit to verify that the Information Security Plan that a supplier's senior management has set is appropriate and in line with good industry practice, and that it has been carried out.

3.16 Our proposal is that this audit is carried out by the CIO. The licence conditions do not specify who in the CIO conducts the audit, as it is considered that this would be a matter for the arrangements between the supplier and the auditor. However the licence conditions define the characteristics of the CIO. The Government considers that requiring independent organisations to conduct these audits instils a high level of confidence that the level of security afforded to smart metering systems can be competently judged and assessed. It is proposed that the first audit should be conducted no later than six months after the licence condition comes into force and then at least once in each subsequent year.

3.17 The draft licence condition requires a supplier's senior management to demonstrate how they have responded to the independent audit report, and such reports could be made available to the Government or the Authority (upon request) to allow it to inform future policy as required.

Role of Government and the Authority (Z.17 to Z.19)

3.18 As noted earlier in this document, the Government is already working with suppliers and other Government agencies to help ensure there is proper preparedness for mitigating risks and taking appropriate actions to manage and operate secure systems. This process will continue. Where it is necessary, the Government proposes that it should have the ability to direct a supplier (or suppliers collectively) to take a particular course of action. This power can be exercised only in the context of achieving secure systems or for the purposes of an appropriate test or trial. The type of scenario where this power might need to be used is where the Government needs to intervene for the purposes of protecting infrastructure. In exercising this power, the Government will consider the available evidence when deciding whether to issue a direction is an appropriate response in respect of particular circumstances.

3.19 During the pre-DCC 'go live' phase, the Government is considering the merits of giving the Authority the power to intervene to ensure that the steps suppliers take with regard to the security of their end-to-end systems will not compromise consumer protection and the functioning of the market. The draft licence condition therefore also provides

[2] HMG's National Technical Authority for Information Assurance
[3] CESG's Certified Professional Mark
[4] CESG's Listed Adviser Scheme
[5] CESG's IT Health Check Service Scheme
[6] CESG's Tailored Assurance Service assessment scheme

for the Authority to have the ability to direct suppliers to take particular steps if necessary. The Government welcomes views on whether it would be an appropriate role for the Authority to make directions in relation to smart metering systems end-to-end security. The Authority will have responsibility for enforcing compliance with the licence condition.

4. Small Suppliers, Domestics and Non-Domestics

4.1 By allowing suppliers to take a risk based approach to security management for SMETS meters deployed during the pre-DCC 'go live' phase, the mitigating controls necessary to ensure a secure end-to-end smart metering system (and therefore costs) are likely to be closely aligned with the type, scale and size of a supplier's operations. However, the Government welcomes views on whether the arrangements for small suppliers, domestic and non-domestic suppliers should be equally applied or whether there are different or other steps that suppliers should take depending on the size of its business or the type of customer it supplies.

5. Security and Smart Meters after the DCC 'Goes Live' (Enduring Security Arrangements)

5.1 The Government, along with stakeholders, is continuing to develop the security governance framework for the period after the DCC starts to provide services. This approach seeks to establish clear accountability of security roles and responsibilities between all participants, and determine who will require assurance that security arrangements have been implemented robustly, and are operating correctly.

5.2 The Government is considering further the appropriate assurance regime that should exist in future, the process of maintaining a set of security requirements, and the technical security arrangements pertaining to future versions of the SMETS, the DCC, and users of DCC.

5.3 This ongoing programme of work considers both smart meters that are operated inside and outside of the DCC and any transitional requirements. The Government plans to consult on the enduring security arrangements in the coming months.

Consultation Questions	
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.***
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?***
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.***

Annex A: Draft Energy Supplier Licence Conditions

Condition Z. Security controls in relation to Smart Metering Systems

Introduction

Z.1 This condition requires the licensee to maintain a high level of security in accordance with good industry practice in relation to all: Smart Metering Systems installed at premises which are from time to time supplied by it with [electricity/gas]; equipment used by it for the purpose of communicating with those Smart Metering Systems; associated software and ancillary devices; and related business processes.

Part A. Application

Z.2 This condition shall have effect until, but cease to have effect on, the date of SEC Go Live.

Z.3 For the purposes of paragraph Z.2, the date of **SEC Go Live** is the date specified in or determined under the Smart Energy Code as being the 'Go Live' date as defined in and for the purposes of that document.

Part B. The general duty to ensure a secure system

Z.4 The licensee must take such steps and do such things as are within its power to provide that the Supplier End-to-End System is at all times Secure.

Z.5 For the purposes of paragraph Z.4, the **Supplier End-to-End System** comprises all of the equipment (together with any associated software and ancillary devices) which falls into one or more of the following categories:

(a) equipment operated by or on behalf of the licensee for the purpose of enabling information to be communicated to or from Smart Metering Systems;

(b) equipment which is a part of any electronic communications network by means of which such communication takes place;

(c) equipment comprised within a Smart Metering System located at each premises that is from time to time supplied with [electricity/gas] by the licensee.

Z.6 For the purposes of paragraph Z.5, the Supplier End-to-End System is **Secure** if both the System and each individual element of it is designed and operated to ensure, to the Appropriate Standard, that it is not subject to interference or misuse that (whether directly or indirectly):

(a) causes any loss, theft or corruption of data;

(b) results in any other unauthorised access to data; or

(c) gives rise to any loss or interruption of [electricity/gas] supply or to any other interference with the service provided to a Customer at any premises.

Part C. Specific duties in relation to a secure system

Z.7 For the purpose of ensuring its compliance with the duty at Part B, the licensee must in particular:

(a) comply with the following requirements of this Part C; and

(b) retain, and produce to the Secretary of State or the Authority when requested to do so, documentary evidence sufficient to demonstrate its compliance with the duty at Part A and, in particular, the requirements of this Part C.

Compliance with Standards

Z.8 The licensee must [take all reasonable steps to ensure that it is able to comply] with the following standards of the International Organisation for Standards with respect to the resilience, reliability and security of the Supplier End-to-End System:

(a) ISO 27001:2005 (entitled *Information Technology – Security Techniques – Information Security Management Systems*); and

(b) any equivalent standard of the ISO that updates, replaces or supersedes that standard.

Information Security Policy

Z.9 The licensee must establish, maintain, and give effect to a policy (the **Information Security Policy**) which must:

(a) be based on a risk assessment in relation to the security of the Supplier End-to-End System; and

(b) set out the manner in which the licensee will operate the Supplier End-to-End System in order to ensure its compliance with the duty at Part B.

Z.10 The Information Security Policy must in particular make appropriate provision for:

(a) measures to mitigate security risks in relation to the Supplier End-to-End System;

(b) restricting access to the Supplier End-to-End System, and to the data communicated over or stored on any element of it, to those who need it and are authorised to obtain it;

(c) the effective management of any security incident on or in relation to the Supplier End-to-End System; and

(d) appropriate business continuity and disaster recovery procedures.

Z.11 The licensee must keep the Information Security Policy under review so as to ensure that it remains appropriate and up to date at all times.

Z.12 The licensee must ensure that the Information Security Policy, and each amendment made to it, is brought to the attention of and considered by appropriate members of its senior management team.

Z.13 The licensee must:

(a) commit adequate levels of resource, including by having a sufficient number of appropriately qualified staff; and

(b) establish all appropriate physical and environmental security controls,

to ensure that it at all times implements the Information Security Policy.

Audit

Z.14 The licensee must:

(a) by no later than [six] months after the date on which this condition comes into force; and

(b) at least once in each subsequent year,

ensure that a security audit of the Supplier End-to-End System is carried out by a Competent Independent Organisation.

Z.15 The licensee must ensure that any audit carried out for the purposes of paragraph Z.14:

(a) includes an assessment of the licensee's compliance with the requirements of Part B and the other requirements of this Part C; and

(b) is documented in a report produced by the auditors and addressed to the licensee, which shall include any recommendations that the auditors consider it appropriate to make as to actions that the licensee should take in order to ensure its compliance with those requirements.

Z.16 The licensee must ensure that:

(a) each report prepared in accordance with paragraph Z.15(b) is brought to the attention of and considered by appropriate members of its senior management team; and

(b) it keeps a written record of the decisions made and actions taken by it in response to that report.

Part D. Compliance with directions

Z.17 The Secretary of State and [the Authority (whether separately or together)] may from time to time issue a direction addressed to the licensee which may require it to:

(a) take (or refrain from taking) such steps as may be set out in the direction for the purposes of:

(i) establishing and maintaining a Secure Supplier End-to-End System for the purposes of any testing and trialling related to the installation or operation of Smart Metering Systems;

(ii) establishing and maintaining a Secure Supplier End-to-End System at all other times;

(iii) mitigating any known or anticipated risk to the security of the Supplier End-to-End System;

(iv) preventing any potential failure of security in the Supplier End-to-End System;

(v) remedying any actual failure of security in the Supplier End-to-End System;

(vi) preparing to address the consequences of any potential failure, or addressing the consequences of any actual failure, in the security of the Supplier End-to-End System;

(b) do so by such a date as may be set out in the direction;

(c) report to the Secretary of State [or the Authority] on the steps that it has taken or will take to comply with the direction;

(d) produce documentary evidence sufficient to demonstrate its compliance with the direction.

Z.18 Any direction issued under this Part D may be addressed to the licensee alone or to the licensee together with any one or more other Gas or Electricity Suppliers.

Z.19 The licensee must comply with any direction issued under this Part D and addressed to it.

Part E. Definitions

Z.20 For the purposes of this condition:

Appropriate Standard means 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.

Competent Independent Organisation means an independent body which is recognised as being qualified to conduct information security audits by virtue of:

(a) employing one or more consultants who are members of the CESG Listed Adviser Scheme (CLAS);

(b) being accredited under the CESG CHECK (IT Health Check Service) Scheme;

(c) being approved as a provider of CTAS

(CESG Tailored Assurance Service) assessments; or

(d) any other membership, accreditation, approval, or similar form of validation that is substantially equivalent in its status and effect to one or more of the arrangements referred to at sub-paragraphs (a) to (c).

For the purposes of this definition, CESG is the National Technical Authority for Information Assurance.

Information Security Policy	has the meaning given in paragraph Z.9.
Secure	has the meaning given in paragraph Z.6.
Supplier End-to-End System	has the meaning given in paragraph Z.5.

© Crown copyright 2012
Department of Energy & Climate Change
3 Whitehall Place
London SW1A 2AW
www.decc.gov.uk

URN 12D/234