Department of Energy & Climate Change

Smart Metering Implementation Programme

Government response to a consultation on a licence condition for security risk assessments and audits in the period before the DCC provides services to smart meters

December 2012

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

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

For further information on this document, contact:
Smart Metering Implementation Programme
Department of Energy and Climate Change
Room 103
55 Whitehall
London
SW1A 2EY

Telephone: 0300 068 4000
Email: Matthew.Adams@decc.gsi.gov.uk

This document can be found on DECC's website:www.decc.gov.uk

Published by the Department of Energy and Climate Change

Introduction

1.1 In April 2012, the Government published its response to the consultation on draft licence conditions and technical specifications for the rollout of gas and electricity smart metering equipment. This included the Government's outline policy for the approach to security arrangements during the period ahead of the Data and Communications Company (DCC) providing services to smart meters.

1.2 In May 2012, the Government invited views on a draft licence condition (on electricity and gas suppliers) giving effect to this policy approach. The consultation closed on 27 July 2012.

1.3 The following questions were posed in that consultation:

- Do you consider that the draft licence condition delivers the policy intention outlined in [the consultation] document?
- 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 [the consultation] document?
- Do you have any further comments with regard to the issues raised in [the consultation] 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 Overall, 15 responses were received. This included all large energy suppliers, a small energy supplier, a number of trade bodies and some communications, data and security specialists. The Government has also continued to work with Ofgem, CESG (National Technical Authority for Information Assurance) and CPNI (Centre for the Protection of National Infrastructure).

1.5 Respondents to the consultation expressed broad support for the policy approach, and agreement that the draft licence condition would deliver this. Beyond this, stakeholders raised points of clarity around some of the specific requirements and some refinements to the draft licence condition.

1.6 Views from respondents on the costs of the approach outlined in the licence condition were in line with our assumptions, and will be reflected in an updated impact assessment. These costs are expected to be proportionate to the size of supplier and number of meters being deployed. The Government considers that the licence conditions should not have any effect on supplier competitiveness, or provide a barrier to new entrants – both of which are key ambitions.

1.7 This document sets out an overview of the Government's proposals and its conclusions in response to comments received through the consultation. A revised licence condition is published at the end of this document to implement the policy approach. Following publication of this consultation response document, the Government expects to lay the licence condition in Parliament and, subject to successful completion of the Parliamentary process, for the licence conditions to take effect in due course. It has a built in sunset clause at the point the DCC provides services – from late 2014 on current planning.

Policy Approach

2.1 The consultation set out the Government's proposals for ensuring security is embedded into the design process for smart meters and their communication systems from the outset. The consultation proposed that this would be delivered through a framework that allows systems and processes to continue to be fit for purpose as security risks, technology, and the requirements continue to evolve.

2.2 The consultation noted that ahead of the DCC 'go live' phase, energy suppliers have end-to-end responsibility for the smart metering solution. This includes their own security assurance regimes (through their procurement, contract, and internal management processes) and whether they deploy equipment which complies with the first 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.

2.3 The draft licence condition outlined an overarching duty on suppliers to ensure a secure system to an 'Appropriate Standard'. To do this, suppliers would 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. The overall aim was to achieve consistency of approach, and to enable suppliers to provide transparency and reassurance to Government and Ofgem that appropriate steps were being taken.

2.4 The following section provides more detail on the key elements of the licence condition and the Government's conclusions in response to comments received during the consultation.

Core Elements of the Supplier Licence Condition

Application (paragraph 2)

3.1 The licence condition was drafted to remain in force during the period until the DCC started to provide services to SMETS compliant meters. The draft licence condition referred to this concept as Smart Energy Code 'Go Live'.

Consultation Outcome and Government Response

Whilst respondents were in agreement that this licence condition should apply for the period up until the DCC starts to provide services to smart meters, there were different points of view as to how this should be captured in the drafting of the obligation. After considering this further, and noting the views of stakeholders, the Government has decided that it is undesirable at this stage to try and define this concept in the drafting of the condition. The Government has therefore chosen a simpler approach, which is to provide for the Secretary of State to issue a direction, in future, to cease the condition. The Government can confirm the intention that this direction will be issued at the point that the DCC starts to provide services to SMETS compliant meters.

It should be noted that after the DCC starts to provide services to smart meters, there will be

different arrangements for security in place for both SMETS compliant meters operated through the DCC and those which a supplier chooses not to enrol in the DCC's services. The Government has recently consulted on this issue[1].

The Government can also confirm that this licence condition only applies to SMETS compliant meters and not to Advanced Domestic Meters (ADM), Automatic Meter Reading (AMR) equipment or other 'smart type' meters.

Secure End-to-End Systems (paragraphs 3 to 6)

3.2 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, the energy supplier's I.T. systems, and all the business procedures associated with the installation, operation and support of the end-to-end system.

3.3. The licence condition states that the system is secure if it is operated to an 'Appropriate Standard'. This standard is further defined in the licence condition.

Consultation Outcome and Government Response

There was broad support amongst respondents for ensuring that suppliers were responsible for security of their end-to-end systems. The licence condition therefore retains this high level obligation. Respondents indicated a preference for some clarity in the legal drafting on the concept of a security incident. A minor amendment has been made to deal with this – making it clear that a security incident is an event of interference or misuse with the supplier end-to-end system or with any individual element of it such that it, for example, causes any loss, theft or corruption of data.

The Government can confirm that suppliers remain responsible for the security of their end-to-end systems even where they make use of service providers. Given this, it is expected that suppliers will make appropriate contractual arrangements when making use of such service providers.

With regard to the definition of the 'Appropriate Standard' a number of respondents considered that it should be made clearer that this related to the energy sector in Great Britain. The Government agrees that this is a useful clarification and has therefore made an amendment to the licence condition.

[1] Smart Metering Implementation Programme: Consultation on the second version of the Smart Metering Equipment Technical Specifications – August 2012

Supplier Information Security Policy: Risk Assessment, Risk Management and Risk Mitigation (paragraphs 7 to 14)

3.4 The draft licence condition set out a number of good practice security disciplines which are expected of suppliers in delivering a secure end-to-end system.

3.5 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. 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.

3.6 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 consultation proposed that suppliers operating SMETS compliant meters in the period before the DCC provides services to smart meters should seek to align their security operations with ISO 27001 during this period, although with no explicit requirement to become certified against this standard.

3.7 The consultation outlined an expectation that suppliers would use this early period to work towards attaining this standard and be able to demonstrate steps they are taking in this regard. The licence condition was drafted to capture this intention, however the consultation invited views on this position.

3.8 The consultation recognised that the risk profile will differ between suppliers but that, 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.

3.9 The Government's proposal was 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 schemes, such as CCP[2], CLAS[3], CHECK [4]or CTAS[5], or a combination thereof.

---

[2] CESG Certified Professional Mark

[3] CESG Listed Adviser Scheme

[4] CESG IT Health Check Service Scheme

[5] CESG Tailored Assurance Service

Consultation Outcome and Government Response

There was support from respondents for implementing a number of good practice security disciplines and that the ones proposed in the licence condition were the right ones. However, the majority of respondents sought greater clarity over what was expected of them with regard to meeting ISO 27001. It was felt that 'working towards' achieving the standard and the way this was drafted in the proposed licence condition was unclear. Respondents felt it could lead to inconsistent approaches between suppliers and, in addition, Ofgem considered it would be difficult to demonstrate that a supplier was taking all reasonable steps to be able to comply with the standard.

The Government wants to give a clear expectation to suppliers and has therefore decided, in line with some of the suggestions in response to the consultation, to give a definite date by which energy suppliers need to be able to demonstrate compliance with the standard. This has been set at eighteen months after the licence condition comes into force.

The Government would also like to highlight that the obligation requires suppliers to comply with ISO 27001 as opposed to requiring them to obtain formal certification against the standard. The Government has chosen this approach because this is a less onerous approach than seeking formal certification. It is in line with an approach of ensuring action is taken which is reasonable and proportionate, and is therefore considered fair to suppliers of any size. It has fewer fixed costs and can be expected to be less costly overall. A supplier will be able to demonstrate compliance through the external audit conducted by a CIO. However, formal certification remains open to suppliers should they wish to seek this.

Independent Audit (paragraphs 15 to 17)

3.10 To provide assurance that risks are being managed in line with the risk assessment and mitigation measures, the consultation proposed that there should be requirements on suppliers to have 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.

3.11 The consultation proposed that this audit should be carried out by the CIO. The draft licence condition did not specify who in the CIO conducts the audit, as it was considered that this would be a matter for arrangements between the supplier and the auditor. However, the licence condition did define the characteristics of the CIO. It was proposed that the first audit should be conducted within six months of the licence condition coming into force, with subsequent audits being carried out at a frequency of at least once in every twelve months. In addition the proposed licence condition required 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 Ofgem (upon request) to allow it to inform future policy as required.

Consultation Outcome and Government Response

Respondents to the consultation were supportive of this approach. Some stakeholders felt that requiring the first audit to be completed within six months was too soon. However, the Government's view is that this deadline should be retained. Requiring an independent audit within the first six months sends a strong signal regarding the importance of security and is important for consumer confidence in smart metering. It will also give suppliers more opportunity to identify and address security weaknesses before they accede to the SEC and begin to enrol meters with the DCC. This approach also reduces the risk that a significant security breach will occur during early rollout. It should be noted that the audit would reflect the size of a supplier's early rollout of smart meters and that the costs of such an audit are therefore expected to be proportionate.

Some changes have however been made to this part of the licence condition as follows:

- Deadline for the Audit Report
    - The Government has specified a time by which the report has to be completed following the audit. This has been set at one month after the audit has been completed.
- Definition of CIO
    - A large number of respondents requested that the licence condition make clear that the lead auditor of the team conducting the audit from the CIO is a member of CLAS. The Government is content to clarify this in the revised licence condition.
    - A small number of respondents suggested that the definition of a CIO should include organisations that employ individuals that hold ISO 27001 Lead Auditor status. Whilst the Government has no objection to CIOs holding this qualification, we do not consider that employing an ISO 27001 Lead Auditor alone should be a qualifying characteristic of a CIO because candidates for the qualification do not undergo a competency based assessment of their skills as information security practitioners. The expectation on suppliers however, is that they will exercise due diligence when appointing auditors to ensure they are capable of conducting the audit.

Overall, the Government remains of the view 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.

Role of Government and Ofgem (paragraph 18)

3.12 The consultation proposed that the Government should have the ability to direct a supplier (or suppliers collectively) to take a particular course of action. It was explained that this power could 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. The consultation further explained that, in exercising this power, the Government will consider the available evidence when deciding whether issuing a direction is an appropriate response in respect of particular circumstances. The Government also invited views on whether the Authority should have such a power of direction outlined in the licence condition.

Consultation Outcome and Government Response

In the main, there was little comment on this section of the licence condition. There were some views expressed about whether there should be some limitations on the Government's power drafted into the licence condition. However the Government notes that such drafting would not be commonplace and, when exercising such a power, it is in any event incumbent on the Government to act reasonably and with due regard to available evidence.

With regard to the role of Ofgem, the Government notes that it already has powers to intervene to protect and facilitate the effective functioning of the energy supply market and to protect consumers. Given this, it is expected that should the need arise, Ofgem can rely on such powers to require suppliers to take a particular course of action.

As noted in the consultation, the Government will continue to work with stakeholders and energy suppliers where appropriate to provide guidance to energy suppliers on the security of smart metering systems.

Conclusion

4.1 Further to the Government's consideration of the responses to the consultation, the licence condition for energy suppliers has been revised. This is attached in an Annex to this document. The Government expects to lay the licence condition in Parliament in October 2012 and, subject to successful completion of the Parliamentary process, the licence condition is expected to take effect by the end of 2012.

Annex A: Licence Condition

Note that Condition 46 relates to electricity supply licence modifications and Condition 40 to gas supply licence modifications.

Condition 46. Security Controls in Relation to Smart Metering Systems

Introduction

46.1 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; 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

46.2 This condition shall cease to have effect from any date specified by the Secretary of State in a direction issued to the licensee under this paragraph.

PART B. THE GENERAL DUTY TO ENSURE A SECURE SYSTEM

46.3 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.

46.4 For the purposes of this condition, 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 by the licensee.

46.5 For the purposes of this condition, the Supplier End-to-End System is **Secure** if both the System and each individual element of it is designed, installed, operated and supported so as to ensure, to the Appropriate Standard, that it is not subject to the occurrence of a Security Incident.

46.6 For the purposes of this condition, a **Security Incident** is any event of interference with or misuse of the Supplier End-to-End System, or with any individual element of it, 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 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

46.7 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 B and, in particular, the requirements of this Part C.

Compliance with Standards

46.8 The licensee must take all reasonable steps to ensure that, by no later than the Specified Date, it complies 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 amends, replaces or supersedes that standard.

46.9 For the purposes of paragraph 46.8, the **Specified Date** is the date which falls 18 months after the date on which this condition comes into force.

Information Security Policy

46.10 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.

46.11 The Information Security Policy must in particular make appropriate provision for:

(a) measures to mitigate the risk of the occurrence of any Security Incident;

(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; and

(d) appropriate business continuity and disaster recovery procedures.

46.12 The licensee must keep the Information Security Policy under review so as to ensure that it remains appropriate and up to date.

46.13 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.

46.14 The licensee must:

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

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

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

Audit

46.15 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 period of 12 months,

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

46.16 The licensee must ensure that any audit carried out for the purposes of paragraph 46.15:

(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 which:

(i) is produced by the auditors and addressed to the licensee;

(ii) is provided by the auditors to the licensee within one month of the completion of the audit; and

(iii) 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.

46.17 The licensee must ensure that:

(a) each report prepared in accordance with paragraph 46.16(b) is considered by appropriate members of its senior management team within four weeks of the report being provided by the auditors to the licensee; and

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

PART D. COMPLIANCE WITH DIRECTIONS

46.18 The Secretary of State 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.

46.19 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.

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

PART E. DEFINITIONS

46.21 For the purposes of this condition:

Appropriate Standard means a high level of security that is in accordance with good industry practice within the energy industry in Great Britain, and is capable of verification as such by a

Competent Independent Organisation.

Information Security Policy has the meaning given in paragraph 46.10.

Competent Independent Organisation means a body which:

(a) is fully independent of the interests of the licensee;

(b) is recognised as being qualified to conduct information security audits by virtue of:

(i) employing one or more consultants who are members of the CESG Listed Adviser Scheme (**CLAS**), or any successor to that scheme;

(ii) being accredited under the CESG CHECK (IT Health Check Service) Scheme, or any successor to that scheme;

(iii) being approved as a provider of CTAS (CESG Tailored Assurance Service) assessments or any successor to those assessments; or

(iv) 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 (i) to (iii), and

(c) has engaged as its lead auditor, for the purposes of the security audit carried out in accordance with paragraph 46.15, an individual who is a member of CLAS or of any successor to or equivalent of that scheme.

	For the purposes of this definition, **CESG** is the National Technical Authority for Information Assurance.
Secure	has the meaning given in paragraph 46.5.
Security Incident	has the meaning given in paragraph 46.6.
Supplier End-to-End System	has the meaning given in paragraph 46.4.”.

Condition 40. Security controls in relation to Smart Metering Systems

Introduction

40.1 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 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

40.2 This condition shall cease to have effect from any date specified by the Secretary of State in a direction issued to the licensee under this paragraph.

PART B. THE GENERAL DUTY TO ENSURE A SECURE SYSTEM

40.3 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.

40.4 For the purposes of this condition, 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 gas by the licensee.

40.5 For the purposes of this condition, the Supplier End-to-End System is **Secure** if both the System and each individual element of it is designed, installed, operated and supported so as to ensure, to the Appropriate Standard, that it is not subject to the occurrence of a Security Incident.

40.6 For the purposes of this condition, a **Security Incident** is any event of interference with or misuse of the Supplier End-to-End System, or with any individual element of it, 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 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

40.7 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 B and, in particular, the requirements of this Part C.

Compliance with Standards

40.8 The licensee must take all reasonable steps to ensure that, by no later than the Specified Date, it complies 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 amends, replaces or supersedes that standard.

40.9 For the purposes of paragraph 40.8, the **Specified Date** is the date which falls 18 months after the date on which this condition comes into force.

Information Security Policy

40.10 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.

40.11 The Information Security Policy must in particular make appropriate provision for:

(a) measures to mitigate the risk of the occurrence of any Security Incident;

(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; and

(d) appropriate business continuity and disaster recovery procedures.

40.12 The licensee must keep the Information Security Policy under review so as to ensure that it remains appropriate and up to date.

40.13 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.

40.14 The licensee must:

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

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

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

Audit

40.15 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 period of 12 months,

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

40.16 The licensee must ensure that any audit carried out for the purposes of paragraph 40.15:

(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 which:

(i) is produced by the auditors and addressed to the licensee;

(ii) is provided by the auditors to the licensee within one month of the completion of the audit; and

(iii) 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.

40.17 The licensee must ensure that:

(a) each report prepared in accordance with paragraph 40.16(b) is considered by appropriate members of its senior management team within 4 weeks of the report being provided by the auditors to the licensee; and

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

PART D. COMPLIANCE WITH DIRECTIONS

40.18 The Secretary of State 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.

40.19 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.

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

PART E. DEFINITIONS

40.21 For the purposes of this condition:

Appropriate Standard	means a high level of security that is in accordance with good industry practice within the energy industry in Great Britain, and is capable of verification as such by a Competent Independent Organisation.
Information Security Policy	has the meaning given in paragraph 40.10.
Competent Independent Organisation	means a body which: (a) is fully independent of the interests of the

licensee;

(b) is recognised as being qualified to conduct information security audits by virtue of:

(i) employing one or more consultants who are members of the CESG Listed Adviser Scheme (**CLAS**), or any successor to that scheme;

(ii) being accredited under the CESG CHECK (IT Health Check Service) Scheme, or any successor to that scheme;

(iii) being approved as a provider of CTAS (CESG Tailored Assurance Service) assessments or any successor to those assessments; or

(iv) 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 (i) to (iii), and

(c) has engaged as its lead auditor, for the purposes of the security audit carried out in accordance with paragraph 40.15, an individual who is a member of CLAS or of any successor to or equivalent of that scheme.

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

Secure has the meaning given in paragraph 40.5.

Security Incident	has the meaning given in paragraph 40.6.
Supplier End-to-End System	has the meaning given in paragraph 40.4.”.

Annex B: List of Respondents to the Consultation

Amethyst Risk Management Ltd

B Global

British Gas

Trilliant

EDF Energy

Energy UK

Energy Services and Technology Association (ESTA)

e.on

First Utility

HP Enterprise Services UK Ltd

Ofgem

Open Web Application Security Project (OWASP)

RWE npower

Scottish Power

SSE

Department of Energy and Climate Change
3 Whitehall Place
London SW1A 2AW
www.decc.gov.uk

URN [12D/395]