ofgem ofgem E-Serve Promoting choice and value for all gas and electricity customers

Smart Metering Implementation Programme: Data Privacy and Security

Document type: Supporting Document

Ref: 94e/10

Date of publication: 27 July 2010

Deadline for response: 28 October 2010

Target audience: Energy suppliers and network operators, consumers, consumer organisations and representatives, environmental bodies, meter asset providers, meter asset managers, meter operators and metering and communication equipment manufacturers, academics and other interested parties

Overview:

This document is one of a number of supporting documents published alongside the Smart Metering Implementation Programme Prospectus.

This document describes the work being undertaken by the programme to deal with data privacy and security. It sets out our proposed principle that consumers should control who has access to their consumption data and the use to which it is put, except where required to fulfil regulatory obligations. Any personal data collected will be protected in accordance with the requirements of the Data Protection Act. We are drawing on a wide range of experience and expertise to ensure we are taking full account of privacy and security issues across the programme.

Contact name: Margaret Coaster

Tel: 020 7901 7000

Email: smartmetering@ofgem.gov.uk

Team: Smart Metering Team, Ofgem E-Serve

Context

The Government is committed to the rollout of electricity and gas smart meters to all homes in Great Britain and to the broad delivery framework underpinning the development of policy to date.

On behalf of the Department of Energy and Climate Change (DECC), Ofgem E-Serve has been managing the first phase of a central programme to design and implement new cross-industry arrangements for the delivery of smart metering. Ofgem E-Serve's smart metering work has been undertaken in conjunction with Ofgem's Sustainable Development Division.

The Prospectus represents the joint views of DECC and the Gas and Electricity Markets Authority (GEMA) based on the work conducted so far during the initial phase of the Smart Metering Implementation Programme ('the programme'). It sets out detailed proposals for consultation on the design and delivery of the smart metering system. Alongside the Prospectus, Ofgem is publishing a number of supporting documents which set out in more detail the alternative options considered.

Reflecting the approach adopted to date, the remaining work to scope the regulatory framework will be led by Ofgem E-Serve on behalf of DECC. Later this year, the governance and management arrangements for subsequent phases of the programme will be decided upon.

Associated Documents

DECC and Ofgem have jointly published the Smart Metering Implementation Programme Prospectus. This document is one of a number of Ofgem supporting documents published alongside the Prospectus.

DECC has also published updated impact assessments for the domestic and non-domestic sectors and a paper on disablement/enablement functionality for smart gas meters.

To help inform the programme, Ofgem also commissioned specific research (carried out by FDS) into consumer awareness of, and attitudes towards, smart metering. All documents are available on the Ofgem website at the following location:

http://www.ofgem.gov.uk/Pages/MoreInformation.aspx?docid=40&refer=e-serve/sm/Documentation

Table of Contents

Summary

Smart metering will deliver significant benefits to consumers by giving them more information and control over their energy usage and by putting an end to estimated billing. The information from smart meters can also be used by suppliers and third parties to help develop innovative tariffs and energy saving advice and by network operators to help manage the gas and electricity networks.

Suppliers currently have access to customers' energy consumption data through conventional and prepayment meters and are used to operating within the framework provided by the Data Protection Act 1998 (DPA). Similarly, network operators are required to have policies and processes in place to ensure the security and integrity of the network is protected at all times.

In developing our proposals for the deployment of smart metering we have placed a strong emphasis on the need to ensure that the additional information smart meters will provide is appropriately controlled and that privacy and security issues are properly addressed.

We are proposing the principle that consumers should be able to choose how their consumption data is used and by whom, except where the data is required to fulfil regulated duties. This principle reflects that being considered by energy regulatory bodies across Europe it is this principle upon which we intend to build our approach to privacy issues.

The proposed principle reflects the objective of the programme to balance concerns regarding any potential intrusion into an individual's privacy with the wider public interest.

The programme intends to work with industry and other stakeholders to assess all of the current and envisaged uses of smart metering data. The programme plans to assess where the data can be provided in an aggregated form and will ensure that it is clear why the data is required. Where customer consent will be required we will look at options for how that consent might be given, including any practical considerations.

Once we are clear on the necessary level of data required to fulfil regulated duties we propose to put in place appropriate governance and the necessary regulatory framework.

To help consumers understand better how smart metering data will be used we are proposing to work with stakeholders to develop a privacy charter. Such an approach is seen as good practice by the Information Commissioner's Office (ICO).

Ensuring the privacy and security of energy consumption data has also been a key consideration in our thinking about the design of the end-to-end smart metering system. Access control will be a core role of the proposed DataCommsCo (DCC). Security requirements are also to be built into the functional requirements that we have developed for the smart metering equipment.

To help develop our thinking we are following a formal security risk assessment approach. We have identified key risks that include unauthorised access to personal data and unauthorised use of remote disconnection functionality. The programme will work with stakeholders to ensure that all risks are appropriately addressed in a way that is proportionate to the risk in terms of upfront investment and ongoing costs.

In line with best practice we will carry out a Privacy Impact Assessment and refine our security risk analysis. The programme is looking to draw on a range of experience and expertise to help us complete this as the overall smart metering system design becomes more certain. In particular we have already established a Privacy and Security Advisory Group drawing on expertise from within government.

We note that some early movers are actively engaging with consumer groups to deal with data privacy concerns. They are also attempting to build flexibility into equipment designs to allow future security upgrades of equipment that has been installed. The programme intends to work with existing early movers to understand how data privacy and security requirements are currently being met.
If early movers are found not to have appropriate data privacy and security measures in place then appropriate action will be taken to ensure compliance. Going forward early movers will be required to bring their arrangements into line with those required by the programme.

While ultimately the responsibility for ensuring privacy and security of the data will sit with the industry parties concerned, the programme will retain a strong focus on this area to ensure that the appropriate obligations are in place and to oversee the arrangements as they are being introduced.

1. Introduction

Context

1.1. The Government is committed to every home in Great Britain having smart energy meters, and consequently empowering people to manage their energy consumption. Businesses and public sector users will also have the opportunity to use smart or advanced energy metering suited to their needs. The rollout of smart metering will play an important role in Great Britain's transition to a low-carbon economy, and help us meet some of the long-term challenges to be faced in ensuring an affordable, secure and sustainable energy supply.

1.2. The Government has also confirmed its commitment to the framework for delivery of rollout including the high-level functional requirements and the need for further consideration of data protection and security.

1.3. We consider that implementing an effective privacy and security framework is central to the programme and we are committed to continuing to engage with consumers, industry and other interested parties to ensure the right balance is struck to protect privacy and confidentiality.

Objectives

1.4. The objectives of this document are to:

- Describe the differences in energy consumption data between conventional and smart metering, and the implications of this in terms of data privacy and security;
- Describe the existing safeguards for data privacy and set out the principle that we intend to adopt in designing the smart metering regulatory regime in relation to privacy issues;
- Explain the importance of security and the approach we are adopting in relation to security issues; and
- Define the next steps that will be taken to integrate principles of data privacy and security within the smart metering system. This includes working with early movers to ensure relevant requirements are being met.

Scope

1.5. This document sets out our approach to data privacy and security for the end-to-end smart metering system. The end to end system covers all equipment, attached devices, communication links and connections from every customer through DCC to suppliers, network operators and third party service providers.

1.6. We discuss the changes in the data captured by smart meters and how this differs from conventional metering. We discuss the current data protection framework and the privacy by design principles that we intend to adopt in designing the smart metering regulatory regime.

1.7. The communication systems that support smart metering must be robust to ensure the potential for deliberate or unintentional interference is adequately addressed. Implementation of appropriate end-to-end security measures are also discussed along with our initial approach in this key area.

Structure of this Document

1.8. This document covers a number of topics:

- Chapter 2 - Background - describes what the change from conventional to smart metering means for available energy consumption data and how this will be provided to industry stakeholders. It provides a summary of the existing data protection framework.
- Chapter 3 - Data Privacy - describes the existing safeguards and the privacy by design principles we intend to adopt in designing the smart metering regulatory framework.
- Chapter 4 - Smart Metering System Security - an explanation of what measures can be used to protect the end to end smart metering system.
- Chapter 5 - Conclusions and Next Steps - enshrining the principles of data privacy and security and working with early movers to understand how data privacy and security obligations are currently being met.
- Appendix 1 - Consultation Response and Questions: sets out the consultation questions raised in this document and how to respond.
- Appendix 2 - Privacy and Security by Design - a short description of the fundamental principles being applied by the programme.
- Appendix 3 - Glossary - of terms used in this document.

2. Background

This chapter explains how data privacy and security requirements will change as a result of the move from conventional to smart metering. The availability of more detailed data raises issues of privacy and intrusion which will need to be considered in deciding what information should be made available. Industry data handling processes will need to change because of the amount of data potentially available and the way it will be communicated throughout the system to industry players.

Information from Conventional Metering

2.1. Where a customer is charged for their gas or electricity on the basis of the quantity supplied then this supply must be measured by an appropriate meter. Conventional meters keep a running total of the energy supplied. Readings are taken normally by a meter reader. By calculating the difference between successive reads the supplier can determine the amount of energy supplied in that period. This information is used to bill the end consumer and on an aggregated basis to determine how much the supplier has to pay through the settlement process for the energy used by their customers overall. The information is stored on suppliers' customer service systems. Network operators currently obtain consumption data, aggregated over numbers of consumers, from suppliers to enable network use of system charging and long term network planning.

2.2. Currently meters are read at a frequency to reflect the needs of the consumer or the supplier which may be as frequently as monthly. In any event suppliers are obliged to take all reasonable steps to read and visually inspect meters at least once every two years. Meter readings may also be provided by consumers to enable more accurate bills. In the absence of a meter reading for a period then the consumer's bill is based on estimated usage. For some electricity customers (on economy 7 tariff) their usage will be measured separately for, typically, two different time periods during the day which have different tariffs.

2.3. Prepayment meters (PPMs) provide greater levels of functionality and data storage capability. With most PPMs there is the ability for meter reading information to be collected and other data downloaded when the customer uses the 'key' to top up their meter. Suppliers are still required to take all reasonable steps to obtain meter readings as part of the two yearly obligation.

2.4. From a security perspective, to date, meter security has been focussed on physical design. This includes measures to prevent fraud through tamper proof fittings and electronics or components designed to provide alerts or evidence when a meter is interfered with.

2.5. As most conventional meters are not connected to a communications system there have not been any risks to the wider gas and electricity infrastructure. More broadly however, it is acknowledged that the industry has a strong security

background and track record at the transmission and distribution level. This provides a foundation to build upon for the required changes for smart metering.

What changes do Smart Meters bring?

2.6. Smart metering will deliver significant benefits to consumers by providing more information and control over their energy usage. This information enables suppliers and third parties to help develop innovative tariffs and energy saving advice. It can also potentially be used by network operators to help in managing the network.

2.7. Smart meters will allow the elimination of estimated bills and prevent the disruption associated with manual meter reading. They will facilitate easier switching between suppliers. Suppliers will be able to offer time-of-use tariffs that should provide consumers with better value for money. For prepayment customers, smart metering will provide new methods and innovative ways of initiating top-ups to their prepayment or pay as you go balance.

2.8. Smart meters will be capable of taking consumption readings every 30 minutes. Other measurement capability will also exist in the metering system to monitor power quality and other key parameters. Our current proposals are that all of this data will be held within the meter – our proposal is that 12 months worth of data can be stored at any one time. Further details can be found in the "Statement of Design Requirements" supporting document.

2.9. In the first instance, for consumers, this information will be available through devices within the home such as the in-home display (IHD). At some stage appliances capable of automatic operation through the Home Area Network (HAN) may also be available.

2.10. There will be the capability for this data to be communicated through the Wide Area Network (WAN) to the proposed DataCommsCo (DCC), and the DCC may then provide the data to authorised third parties. Access and authorisation rights to allow the disclosure of data are discussed in Chapter 3. Further details of the DCC and its role and responsibilities can be found in the "Communications Business Model" supporting document.

2.11. Smart metering also provides the possibility that more energy consumption data will be held by third parties, inside and outside of the energy supply chain, than currently. One example of this is that smart meters will allow, where the consumer agrees, energy management and efficiency companies to use energy consumption data in order to provide tailored packages to consumers.

2.12. The availability of this detailed information from smart meters is particularly beneficial because:

- Customers will be able to make informed decisions about energy consumption;

- As the meter reads, stores and transmits this data electronically this helps to remove the need for manual meter readings and estimated bills;
- Suppliers can enhance customer service and billing processes;
- Network operators can improve methods of system charging, actively manage networks, such as supply outage management, and enhance network planning; and
- Other energy services companies can offer services and advice to assist consumers in reducing energy consumption.

2.13. Prepayment services will also be managed remotely. This will allow consumers to add credit to meters through new methods, such as the internet or by telephone and where cash payment is made this can be done without having to use physical media such as cards or keys.

2.14. There is clearly a significant shift in the amount of data available and the method of providing this to consumers and other interested industry participants and third party service providers. It is our initial view that the detailed data that can be collected through smart meters has the potential to reveal information about a consumer's lifestyle and habits and there is potential to breach the Data Protection Act if personal data is not handled properly. Controls therefore need to be in place to ensure that industry and third parties manage data correctly and that consumers have appropriate rights and are sufficiently protected.

2.15. The change to electronic communication provided through the introduction of smart meters also presents a new risk to be managed by operators of the gas and electricity infrastructure. All smart electricity meters and smart domestic gas meters will be fitted with the capability to enable and re-enable supply. Each device connected to a HAN will be a potential interface to the overall smart metering system. We will ensure that the end-to-end smart metering system is sufficiently protected to ensure that the infrastructure is not compromised.

Data Privacy Framework

2.16. Data privacy is primarily regulated in the UK by the Data Protection Act 1998 (DPA), which implements the EU Data Protection Directive[1]. The DPA is enforced by the Information Commissioner's Office (ICO).

2.17. The DPA establishes a framework of rights and duties which are designed to safeguard personal data. This framework balances the legitimate needs of organisations to collect and use personal data for business and other purposes against the right of individuals to respect for their privacy and to control their personal details. The legislation is underpinned by eight data protection principles which may be broadly summarised as:

[1] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

- Personal data must be fairly and lawfully processed;
- Personal data must be obtained only for specified and lawful purposes, and must not be further processed in a manner which is incompatible with that purpose;
- Personal data must be adequate, relevant and not excessive in relation to the purpose for which it is processed;
- Personal data must be accurate and, where necessary, kept up to date;
- Personal data processed for any purpose must not be kept for longer than is necessary for that purpose;
- Personal data must be processed in accordance with the person's rights under the DPA;
- Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data; and
- Personal data must not be transferred outside the European Economic Area unless that country or territory ensures an adequate level of protection in relation to the processing of personal data.

2.18. The DPA applies to the processing of personal data. This means that where a person processes personal data they must comply with the DPA and in particular handle the personal data in accordance with the data protection principles.

2.19. As pointed out by the ICO, it is important to be aware that energy consumption data may be personal data where a living individual can be identified either from the energy consumption data itself or from the energy consumption data and other information in the possession of a person, such as a name and address held for billing purposes. Where these requirements are satisfied, energy consumption data will be personal data for the purposes of the DPA regardless of whether the energy consumption data is obtained from a conventional meter, prepayment meter or smart meter.

2.20. Smart meters will allow for energy consumption data to be recorded and stored at a greater level of detail than that provided by current conventional or prepayment meters. The programme recognises that this more detailed energy consumption information may provide more detailed information about a person's lifestyle. It also recognises the potential for this to raise concerns about the intrusion of an individual's privacy. The programme has therefore reviewed its proposals to date to ensure compatibility with the European Convention on Human Rights (ECHR) and will continue to do so as its proposals are developed in further detail.

2.21. The programme has also reviewed its proposals to date to ensure compatibility with the key principles underlying the EU Data Protection Directive[2] and will continue to do so as its proposals are developed in further detail.

[2] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

Learning and benefiting from experience

2.22. The programme has followed closely a number of other smart metering programmes where privacy and security issues have been reported.

2.23. In the Netherlands a consumer body raised concerns about the privacy implications of the national smart metering programme and specifically about whether the programme had the potential to contravene the European Convention on Human Rights (ECHR). The Government of the Netherlands has modified its smart metering programme to address the privacy concerns raised. We have closely reviewed the privacy issues raised in relation to the Dutch smart metering programme and have taken these into account in developing our approach.

2.24. The programme has sought engagement with relevant international expert groups and standards bodies. In the USA the National Institute of Standards and Technology (NIST) is developing a set of interoperability requirements which directly address privacy and security issues. A number of other working groups are focussed on other privacy and security topics. The programme is linked into these key groups.

2.25. In Europe, the EU Commission has formed an Expert Group as part of the Smart Grid Task Force initiative to focus on the privacy and security issues relating to smart grids. The programme was represented in this working group. Additionally the European Regulators' Group for Electricity and Gas (ERGEG) is also developing smart grid guidance, some of which addresses privacy and security issues.

2.26. The programme has engaged with the ICO, the Centre for Protection of National Infrastructure (CPNI) and other government organisations that have a role in relation to, or experience of, data privacy or security within the UK. The programme has also engaged with private sector security specialists and test houses.

2.27. The programme has considered the Online Targeting of Advertising and Prices market study recently published by the Office of Fair Trading[3]. Whilst this investigates online internet practices there are potential lessons in relation to electronic communications and data capture. This will continue to inform our thinking moving forward into the next phase of the programme.

2.28. The programme recognises the significance of privacy and security. We have developed our approach to ensure these risks are addressed appropriately in the overall design of the smart metering system. The programme will influence relevant industry participants to provide solutions through functional and technical requirements. These will be proportionate to risk in terms of upfront investment and ongoing costs. The experience of other deployments has reaffirmed our view that building data privacy and security at design is essential to the success of the programme. Further design detail can be found in the "Communications Business Model" and "Statement of Design Requirements" supporting documents.

[3] *Online Targeting of Advertising and Prices: A market study*, Office of Fair Trading, May 2010.

2.29. The programme has sought to learn from the experience gained elsewhere in the world. Building on this we are looking to introduce robust arrangements to ensure that consumers can have confidence that security and data privacy are integral parts of the rollout of smart metering in Great Britain.

2.30. There is a need to ensure that the initial requirements to provide security and data privacy keep pace with the development of technology and of smart grids. We will continue to look at the best way to ensure that the impact of these developments on privacy and security are proactively managed.

3. Data Privacy

This chapter discusses data handling and the approach to maintaining privacy. The chapter then proposes an approach for consideration.

Question 1: Do you have any comments on our overall approach to data privacy?

Question 2: We seek views from stakeholders on what level of data aggregation and frequency of access to smart metering data is necessary in order for industry to fulfil regulated duties.

Question 3: Do you support the proposal to develop a privacy charter?

Question 4: What issues should be covered in a privacy charter?

Existing Safeguards

3.1. Data privacy is regulated in Great Britain by the DPA. Industry participants must currently comply with the DPA when processing personal data, which may include energy consumption data from conventional meters and PPMs and in particular must handle any such personal data in accordance with the eight data protection principles established by the DPA.

3.2. We therefore expect industry participants to already be aware of, and comply with, all applicable obligations under the DPA, and to have appropriate policies and procedures established to achieve this. We will expect industry participants to comply with their obligations under the DPA when processing any energy consumption data from smart meters that may be regarded as personal data under the DPA, as they do now for other personal data about consumers obtained from other sources, for example, contact details and credit card details.

Privacy by Design

3.3. In addition to complying with the existing rules under the DPA, the programme intends to consider privacy needs prior to the development of systems and processes by adopting privacy by design principles[4] throughout the smart metering regulatory regime. The programme recognises the confidentiality issues that may arise with respect to energy consumption data for non-domestic consumers and we propose that privacy by design principles should apply to both domestic and non-domestic consumers.

3.4. A 'privacy by design' approach ensures that privacy issues are identified at the earliest stages of the programme. This allows us to mitigate risks in a variety of ways. Within the different areas of the programme this has influenced thinking around minimising data collection, anonymising data where practicable, agreeing

[4] Please see Appendix 2 for a description of privacy by design.

data handling practices and ensuring data privacy and security is included in the detailed design of the system. For example, we have a functional requirement for the meter to be built as the primary store of smart metering data, because in the first instance, the meter will allow consumers to understand their energy consumption as the meter, which communicates with the consumers' in home display (IHD), will have the ability to store twelve months' worth of data.

3.5. This ongoing approach is intended to produce an effective privacy solution and minimise overall costs. We will continue to follow privacy by design principles as we develop the smart metering regulatory regime.

3.6. In order to deliver 'privacy by design' we will build on our initial work to carry out a detailed privacy impact assessment (PIA). We are using the PIA approach and, through an iterative process, this will influence policy developments relating to privacy across the programme. As the PIA develops this will inform the options for the Smart Metering Implementation Programme.

3.7. One of the key features of our 'privacy by design' strategy is our approach to data handling issues which are discussed in more detail below.

Data control and access rights

3.8. Smart meters enable a much more detailed level of energy consumption data to be captured. The increased frequency of readings may produce more information about people's lifestyle and habits, so necessary safeguards need to be in place. It is important that organisations capturing the data have a lawful basis to do so and clearly inform consumers why their data is being captured and for what purpose. Additionally, only data that is necessary for the lawful purpose should be captured and data should not be held onto for longer than necessary.

3.9. One of the key questions for the programme is to determine who has rights to access the data - and for what purpose.

3.10. Data may be grouped together or aggregated. This aggregation could be across a number of consumers' consumption information or the bringing together of frequent readings from one consumer's meter.

3.11. We have listened to the views of a broad range of stakeholders on this key issue. In light of our discussions, we propose that **the consumer should choose in which way consumption data shall be used and by whom, with the exception of data required to fulfil regulated duties**. This aligns our approach to that being proposed by ERGEG (the group of European energy regulators) in guidance being developed for smart metering[5].

[5] *An ERGEG Public Consultation Paper on Draft Guidelines of Good Practice on Regulatory Aspects of Smart Metering for Electricity and Gas*, ERGEG, June 2010.

3.12. We recognise that industry will require access to a certain amount of smart metering data which is required in order for industry to fulfil regulated duties. It also recognises that the data that industry requires may relate to an individual consumer or may be aggregated across a number of consumers in such a way that it is not possible to link it to an identifiable individual.

3.13. We seek views from stakeholders on what smart metering data, including the level of aggregation and frequency of it being recorded, should be considered as being required by industry to enable them to fulfil their regulated duties. We would also like to understand where industry participants and interested third parties may wish to have access to information for other purposes, subject to consumer consent as necessary. The programme will consider the information provided and will work with stakeholders to develop a more detailed understanding of these requirements and the privacy issues they raise.

3.14. As part of this work the programme will need to consider the value of data in helping the Government to analyse the effectiveness of its policies and in the production of official statistics.

3.15. The operational requirements to facilitate the best outcome for the programme will also need to be developed. We acknowledge that requiring customers to opt in to provide data may lead to limited numbers of customers allowing access to the data which could undermine some of the benefits. Conversely, allowing opt out would ensure wider availability of data but will raise issues around ensuring informed consent and questions as to whether that provides adequate protection. While it may be appropriate to specify different levels of control (opt in or opt out) for different categories and uses of data it is important that the arrangements do not become overly complex for consumers.

3.16. Clear information about the rights of consumers with respect to their consumption data, for example access to data, the right to rectify certain data and to consent to the disclosure of data, should be available. Where consumers are provided with the option to consent to a disclosure, they should be given full opportunity to be made aware of the implications of providing consent as well as the methods for withdrawing consent.

3.17. There are also other practical issues to be confronted. We recognise that network companies have no direct consumer relationship and we will need to consider the route to follow for such parties to gain consumer consent to disclosure of data.

3.18. There is a need to ensure that the rollout of smart metering does not create an unwelcome level of intrusion into individuals' private lives. The principle that the customer should determine who has access to their consumption data beyond that which is required to fulfil regulatory duties should ensure that the consumer has the ability to select the level of information that is provided to external parties, and therefore limit any unwelcome or unnecessary privacy intrusion.

Data use

3.19. The data collected through smart meters must be used for legitimate purposes and all industry participants must be able to demonstrate clearly the purposes for which they wish to use the data. As part of safeguarding privacy, all participants should only use the data for the purpose for which it was collected and not for some secondary purpose. If the participant has not obtained the data directly from the consumer, it is necessary for the participant to ensure that it has a lawful basis upon which to use the data and that consumers are properly informed about how their data will be used.

Data storage

3.20. Due to the potential sensitivity of the data obtained through smart meters it is vital that data is held in appropriately secure conditions. We set out our approach to security in more detail in Chapter 4. Alongside putting in place appropriate security measures, industry participants should not hold onto data for longer than is necessary and should implement regular deletion or anonymisation procedures.

Data sharing

3.21. One of the benefits of the programme is the ability for data to be accessed by different parties. In line with our comments above about data control, such disclosures would be in the hands of the consumer. The consumer would determine whether he wished to share data with an industry participant or interested third party, except where the data is required to fulfil regulated duties.

3.22. As noted above, we would like to understand in what circumstances and why industry participants and interested third parties may wish to have access to information . The programme will consider the information provided and will work with stakeholders to develop a more detailed understanding of these requirements and the privacy issues they raise.

Data access

3.23. Through the in-home display, consumers will be able to access directly consumption data collected through the smart meter. It is important for purposes of transparency as well as protecting individuals' rights that consumers are able to access their data. Additionally, industry participants and interested third parties must provide consumers with details on how the consumer can access data held by such participants and interested third parties.

3.24. We will continue to develop our proposals in consultation with stakeholders, and in particular seek views on the proposed approach. We will also consider whether any specific licence obligations should be imposed upon licensees in order to implement our proposals with respect to data privacy. Where this occurs, Ofgem will

discuss appropriate arrangements with the ICO, and will consider whether there is a need for a Memorandum of Understanding between them, to provide clarity on their respective roles in this area.

Question 1: Do you have any comments on our overall approach to data privacy?

Question 2: We seek views from stakeholders on what level of data aggregation and frequency of access to smart metering data is necessary in order for industry to fulfil regulated duties.

Privacy charter

3.25. To help consumers better understand how the smart metering data will be used and to set out to all participants of the programme how smart metering data should be used, we are proposing to work with stakeholders to develop a privacy charter. Such an approach is seen as good practice by the ICO.

3.26. A privacy charter would set out principles to address privacy concerns associated with the rollout of smart metering. A charter would complement the legally binding principles of the DPA and help make the messages more accessible for consumers. The programme considers that this could be an important means of providing consumers with assurance in this area. We seek views from stakeholders on whether to develop a privacy charter and what points should be covered.

Question 3: Do you support the proposal to develop a privacy charter?

Question 4: What issues should be covered in a privacy charter?

4. Smart Metering System Security

This chapter discusses the approach the programme has adopted to securing the smart metering system. It includes liaison with experts in government, the security sector and industry. The initial risk assessment method and initial outputs are discussed. This chapter also shows where the programme believes security responsibilities will fall across the smart metering system.

Question 5: Do you agree with our approach for ensuring the end-to-end smart metering system is appropriately secure?

Informed Approach

4.1. Security of the smart metering solution is paramount to ensuring consumer confidence in the programme. The evolution of meters which can communicate with other devices in the home and support receipt and sending of remote communications necessitates careful consideration of the associated security requirements. This is important to ensure consumer protection and the effective operation of the energy industry.

4.2. We have held, and will continue to hold, discussions with a number of parties to assist in developing our understanding of the requirements and to determine our process for delivering security. These parties include:

- Office for Cyber Security;
- Centre for the Protection of National Infrastructure;
- Communications-Electronics Security Group;
- Specialist smart meter and smart grid testing organisations;
- Private sector security specialists;
- Suppliers and Network Operators; and
- Meter vendors.

4.3. This liaison has influenced the approach we have taken to an initial security risk assessment. We note that there are measures already in place to protect the gas and electricity infrastructure at the transmission and distribution level and will seek to harness that expertise and, where appropriate, build upon the existing framework.

4.4. We have adopted security by design principles that are closely aligned to privacy by design[6]. This ensures that security is built into the smart metering systems and processes from the start of the programme. Security is needed both to protect the privacy and integrity of data within the end-to-end system and protect the services provided by the systems. The security requirements will inform the design of the system, where data is stored and the obligations that government will place upon participants in the end-to-end system. To do this we will assess the risks to the end-

[6] Please see Appendix 2 for a description of privacy by design.

to-end system. Security by Design is more fully described in Appendix 2 of this document.

Risk Assessment

4.5. We have adopted a risk based approach for the identification of security issues. We will have appropriate security measures in place so that security is properly reflected within the design of the end-to-end smart metering system in future programme phases. Data privacy and security aspects will be integrated into the emerging technical specifications for the system design and all relevant aspects of DCC operation and management.

4.6. We have adopted a risk management methodology that follows the Government's Security Policy Framework and Information Assurance processes. An initial Information Assurance Standard No. 1[7] risk assessment has been undertaken. This has identified the potential threats, likelihoods, impacts and vulnerabilities for the emerging options for the end-to-end smart metering system.

4.7. At this stage in the programme the overall design of the smart metering system solution is not yet finalised. We intend to refine the risk assessment, in increasing detail, as options become firmer, to inform decisions to be made on system design. The output from this process will inform the programme's thinking, including the process of developing technical specifications under the expert groups as described in the "Implementation Strategy" supporting document. We intend to continue to engage appropriate security specialist expertise to assist the programme in ensuring that security requirements are defined and put in place for the complete end-to-end system.

4.8. The initial risk assessment has identified the key risks. Key risks include unauthorised access to personal data and unauthorised use of remote disconnection functionality. These are risks that are common to smart meter and smart grid programmes across the world. The programme will continue to monitor developments in other programmes and work with EU colleagues to determine appropriate and consistent policy and standards for addressing risks.

4.9. Our intention is to share our risk assessment output with relevant stakeholders, under appropriate controls, as we move forward. In relation to the vulnerabilities detected, the programme will ensure that mitigating actions are put in place by relevant parties so that potential threats are appropriately addressed.

4.10. Government will put in place technical and organisational measures to ensure that the system addresses risks identified from the risk assessment in a proportionate manner. We have considered measures to address risks that may be derived from deliberate or unintentional actions. These measures include:

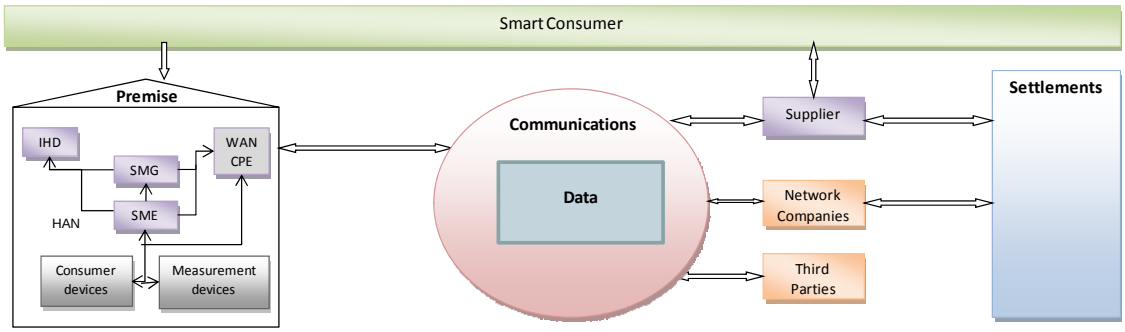
[7] *HMG IA Standard No. 1 Technical Risk Assessment*, CESG, October 2009.

- Ensuring that smart metering equipment installed in premises and communication equipment in the wider area are appropriately protected from physical and electronic tampering;
- Ensuring the devices, such as the IHD or other equipment connected to the HAN, cannot be misused or be used as a "backdoor" into the metering system;
- Utilising secure communications to prevent eavesdropping, interception and modification of data;
- Ensuring that robust authentication and access control mechanisms are used;
- Requiring stringent security testing;
- Ensuring that security events are detectable and that incidents can be managed appropriately; and
- Providing appropriately targeted and regular training to personnel about security.

Security Requirements

4.11. The outputs of the initial risk assessment have been considered in the context of the 'end to end' system shown in Figure 1. A number of risk mitigation measures have been considered from a variety of sources including the HMG Security Policy Framework (Information Assurance Standard No. 1), NIST guidance, USA Department of Homeland Security Requirements and industry best practice. In developing security the programme will continue to work with security experts and the CPNI utility industry security groups.

Figure 1 - The end-to-end smart metering system



4.12. The following points are the areas of potential threat and risk:

- Home devices;
- Microgeneration devices (such as solar panels and domestic wind turbines);
- Communication links between home devices and the smart meter;
- The smart meter;
- Communications links between the smart meter and DCC;
- DCC;
- Communication links between DCC and suppliers, network operators and third parties; and
- Suppliers, network operators and third parties.

4.13. On the basis of these potential risks, the programme will develop a privacy and security compliance framework to ensure:

- Integrity and availability of the data transferred across wireless communications is maintained;
- Metering and communications equipment is tamper proof and has appropriate tamper alarms;
- Meters are only accessed by authorised persons and only for those activities for which they are authorised, through appropriate security controls;
- Meters can resist infiltration from unauthorised access and have their software updated to prevent emerging risks;
- Assurance around the development and maintenance of metering systems; and
- Authorised data controllers protect data and access to data that has been communicated from the meter.

Sector responsibilities

4.14. The core responsibilities for industry participants will include:

- Equipment manufacturers and technology providers: Ensuring products comply with security standards that form part of the functional requirements and technical specifications.
- Supply licensees: Ensuring that equipment installed and managed complies with security standards, the installer of metering equipment within customer premises is appropriately trained and vetted and all access permissions are adequately controlled.
- Other third parties: Access to data is appropriately controlled to data authorised and managed on an ongoing basis.
- DCC licensee: Ensuring an appropriate security model is implemented to protect data communications and processing including appropriate access control, staff vetting/competence training and security response and incident management.

4.15. This list is not intended to be exhaustive, and other responsibilities are present, but it does show the areas where industry will need to develop management and systems going forward to meet the security requirements. An initial view of security requirements for metering equipment have been considered and can be found in the "Statement of Design Requirements" supporting document.

4.16. It is noted that the DCC will play an important role in ensuring the security of the end-to-end system. This will include elements of meter data management, connection to suppliers and incident management. This security model will be built into the design of technical specifications and DCC as it develops. Further detail can be found in the "Statement of Design Requirements" and "Communications Business Model" supporting documents.

4.17. The next phase of the programme will focus on updating the risk assessment and developing the assurance and accreditation process to establish an end-to-end

security model in line with the Security Policy Framework and security standards such as ISO 27001[8].

Question 5: Do you agree with our approach for ensuring the end-to-end smart metering system is appropriately secure?

[8] ISO/IEC 27001:2005 Information technology -- Security techniques -- Information security management systems – Requirements.

5. Conclusions and Next Steps

This chapter details the future work and approach the programme intends to take forward into the next phases of the programme. This includes working with early movers, developing the PIA and security risk assessment and utilising the guidance and experience of the Privacy and Security Advisory Group.

Summary of proposals

5.1. A number of proposals set out in this document are summarised below:

- The rollout of smart metering will adopt privacy and security by design;
- The privacy and security compliance framework will include the principle that consumers should be able to choose how their consumption data is used and by whom except where the data is required to fulfil regulated duties;
- The programme will build on our initial work to develop a full PIA and security risk assessments to embed data privacy and security into the smart metering system design in a manner that is proportionate to the level of risk identified;
- The functional requirements and technical specifications will include security requirements;
- The programme will work with industry to embed security solutions into smart metering equipment and communications that are proportionate to the identified risks; and
- The programme will develop a privacy charter to reflect the principles above and reflect DPA obligations for the sector.

Future work

5.2. Data privacy and security remains a key focus of the programme and we believe it is essential that all industry participants actively engage to ensure that the integrity of the smart metering system is robust and that consumer confidence is maintained in the transition to smart metering.

5.3. Implementation of smart metering requires a step change in the approach to data privacy and security. We welcome the fact that some early movers are actively engaging with consumer groups on data privacy concerns and are attempting to build flexibility into equipment designs to allow security to be upgraded when equipment is in use. If early movers are found not to have appropriate data privacy and security measures in place then appropriate action will be taken to ensure compliance. Going forward they will be required to bring their provisions into line with the necessary requirements.

5.4. We are acting to ensure that privacy and security are fully considered within all aspects of the smart metering regime. This work will continue to evolve into the next phases of the programme. Our initial work on a PIA will further develop alongside progression of the security risk assessment.

5.5. The programme will be reviewing all existing regulatory arrangements relating to access to and use of energy consumption data to ensure that they remain appropriate for a smart metering environment.

5.6. We will work with industry through the next phases of the programme to build on the knowledge that they have gained from decades of protecting the energy infrastructure and consider whether this can be adapted for use when smart metering is implemented. Compliance with security and technical standards, potentially under accreditation, is a widely accepted assurance process that could form part of our future security strategy.

5.7. The programme will maintain a strong oversight role in this crucial area and will engage proactively with relevant industry participants as development of the programme progresses.

5.8. The programme will continue to engage with all stakeholders in our work and will engage with privacy experts and ensure a clear consumer voice in developing the data privacy policy and charter.

Privacy and Security Advisory Group

5.9. In line with best practice we have established a Privacy and Security Advisory Group (PSAG) to provide advice and guidance in this key area to ensure that the programme achieves a fair balance in its approach. PSAG currently comprises representatives from other areas of government where expertise and experience exists with data privacy and security, including representatives from the ICO and the CPNI. We are considering the expansion of the advisory group to include external stakeholders.

5.10. The programme will continue to develop best practice from the experience gained by similar projects both in this country and overseas. The programme will also maintain close working relationships with relevant government bodies. Our aim is to ensure that the programme is at the forefront of developments in this key area and to ensure that confidence is maintained across the spectrum of interested parties.

Appendices

Index

Appendix 1 – Consultation Response and Questions

1.1. We would like to hear the views of interested parties in relation to any of the issues set out in this document. When responding please state whether you are responding as an individual or representing the views of an organisation. If responding on behalf of an organisation, please make it clear who the organisation represents and, where applicable, how the views of members were assembled.

1.2. We would especially welcome responses to the specific questions included in each chapter and that are replicated here. These detailed questions sit behind the more high-level questions contained in the Prospectus.

1.3. Responses should be received by **28 October 2010** and should be sent to:

- Margaret Coaster
- Smart Metering Team, Ofgem E-Serve
- 9 Millbank, London SW1P 3GE
- 020 7901 7000
- smartmetering@ofgem.gov.uk

1.4. Unless marked confidential, all responses will be published by placing them on the websites of Ofgem (www.ofgem.gov.uk) and DECC (www.decc.gov.uk). Respondents may request that their response is kept confidential.

1.5. Respondents who wish their responses to remain confidential should clearly mark the document(s) to that effect and include the reasons for confidentiality. Respondents are asked to put any confidential material in the appendices to their responses. It would be helpful if responses could be submitted both electronically and in hard copy.

1.6. Individual responses and information provided in response to this consultation, including personal information, may be subject to publication or disclosure in accordance with the access to information regimes (these are primarily the Freedom of Information Act 2000 (FOIA), the Data Protection Act 1998 (DPA) and the Environmental Information Regulations 2004).

1.7. In view of this, 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 as binding on the Department of Energy and Climate Change or Ofgem. We will process your personal data in accordance with the DPA. In the majority of circumstances, this will mean that your personal data will not be disclosed to third parties.

1.8. Any questions on this document should, in the first instance, be directed to:

- Margaret Coaster
- Smart Metering Team, Ofgem E-Serve
- 9 Millbank, London SW1P 3GE
- 020 7901 7000
- smartmetering@ofgem.gov.uk

1.9. You may make copies of this document without seeking permission. Further printed copies of the consultation document can be obtained from the contact above. An electronic version can be found on the Ofgem website at: www.ofgem.gov.uk. Other versions of the document in Braille, other languages or audio-cassette are available on request.

CHAPTER 3

Question 1: Do you have any comments on our overall approach to data privacy?

Question 2: We seek views from stakeholders on what level of data aggregation and frequency of access to smart metering data is necessary in order for industry to fulfil regulated duties.

Question 3: Do you support the proposal to develop a privacy charter?

Question 4: What issues should be covered in a privacy charter?

CHAPTER 4

Question 5: Do you agree with our approach for ensuring the end-to-end smart metering system is appropriately secure?

Appendix 2 – Privacy by Design and Security by Design

1.1. As part of our work in this area we recognise that security and privacy are best dealt with by designing them into systems from their inception. For technical solutions, such as the end-to-end smart metering system this ensures that they are robust and can provide cost savings over dealing with these aspects in a reactive way.

1.2. Stakeholders have endorsed this approach and support our commitment to ensuring the end-to-end smart metering system is robust by adopting the concepts of privacy by design and security by design.

Security by design

1.3. Security by design is defined as ensuring that the security of a system is designed from the ground up to be secure. Security by design is an established concept where security risks and issues are identified early in the system's development lifecycle. Often this approach allows security issues to be designed out of a system or effective controls to be established, therefore maximising efficiency and reducing costs.

Privacy by design

1.4. Privacy by design is described by the ICO as a concept that encourages organisations to give due consideration to privacy needs prior to the development of any new system or process, and to maintain that control throughout the end-to-end system's lifecycle. This lifetime approach ensures that privacy controls are stronger, simpler to implement, harder to bypass, and totally embedded in the system's core functionality[9]. A system that has been designed with privacy in mind from the outset provides better privacy protection that is often simpler and more cost effective than trying to bolt on privacy protection at a later date.

1.5. We are ensuring that privacy by design is embedded in the smart metering programme by:

- Carrying out a privacy impact assessment (PIAs) and encouraging industry to carry out their own PIAs for their own internal systems.
- Establishing a privacy charter, which will aid the development of cross-sector standards for data sharing.

[9] Privacy by design ICO website: http://www.ico.gov.uk/upload/documents/pdb_report_html/index.html

Appendix 3 – Glossary

A

Access control

The method used to ensure that access to meter data is only available to properly authorised parties.

C

Codes

Industry codes establish detailed rules that govern market operation, the terms for connection and access to energy networks. The supply and network licences require the establishment of a number of industry codes that underpin the gas and electricity markets. The electricity codes are: Balancing and Settlement Code (BSC), Connection and Use of System Code (CUSC), Distribution Code, Grid Code, Master Registration Agreement (MRA), System Operator-Transmission Owner Code (STC) and Distribution Connection and Use of System Agreement (DCUSA). The gas codes are the Uniform Network Code (UNC), Independent Gas Transporter (IGT) Network Codes, Supply Point Administration Agreement (SPAA).

Commercial interoperability

The terms on which a new supplier can use the meter and related equipment when a customer changes supplier.

Consumer

Person or organisation using electricity or gas at a meter point.

Customer

Any person supplied or entitled to be supplied with electricity or gas by a supplier.

D

DataCommsCo (DCC)

New proposed entity which would be created and licensed to deliver central data and communications activities. DCC would be responsible for managing the procurement and contract management of data and communications services that will underpin the smart metering system.

Data Protection Act 1998

The Data Protection Act 1998 defines UK law on the processing of data on identifiable living people. It is the main piece of legislation that governs the protection of personal data in the UK.

Department of Energy and Climate Change (DECC)

The Department of Energy and Climate Change (DECC) was created in October 2008, to bring together: energy policy and climate change mitigation policy.

E

Electricity meter

A measuring instrument that records the quantity of electricity supplied.

Energy suppliers

A company licensed by Ofgem to sell energy to, and to bill, customers in Great Britain.

Estimated bills

Where a supplier is unable to obtain a meter reading, a customer's bill will be estimated based on past usage.

F

Functional requirements

The minimum functions that must be supported by the different elements of the smart metering system to ensure the delivery of the benefits of smart metering. Describes what the smart metering system must do (not how it must do so).

G

Gas meter

A measuring instrument that records the volume of gas supplied.

H

Home Area Network (HAN)

The smart metering HAN will be used for communication between smart meters, IHDs and other devices in consumers' premises.

I

In-home display (IHD)

An in-home display is an electronic device, linked to a smart meter, which provides information on a customer's energy consumption.

L

Licence

Transporting, shipping and supplying gas; and generating, transmitting, distributing and supplying electricity are all licensable activities. Ofgem grants licences that permit parties to carry out these activities in the GB market. The licenses require the establishment of a number of multilateral industry codes that underpin the gas and electricity markets. Licensees need to be signed up as parties to codes in order to operate in the gas and electricity markets (see codes).

M

Microgeneration

Microgeneration is the on-site generation of lower carbon heat and power by individuals, small businesses and communities at a small scale.

N

Network operators

The companies that are licensed by Ofgem to maintain and manage the electricity and gas networks in GB.

O

Ofgem

The Office of the Gas and Electricity Markets (Ofgem) is responsible for protecting gas and electricity consumers in Great Britain. We do this by promoting competition, wherever appropriate, and regulating the monopoly companies that run the gas and electricity networks.

Ofgem E-Serve

Ofgem E-Serve is responsible for Ofgem's support and delivery functions. It focuses on administering environmental programmes and the delivery of sustainability projects such as the Smart Metering Implementation Programme.

P

Prepayment meter (PPM)

These are meters that require payment for energy to be made in advance of use or else they will prevent the supply of gas or electricity. A PPM customer pays for energy by inserting electronic tokens, keys or cards into the meter.

Privacy by design

A system that has been designed with privacy in mind from the outset.

Programme

The Smart Metering Implementation Programme.

S

Security by design

Security by design is defined as ensuring that the security of a system is designed from the ground up to be secure. It is an established concept where security risks and issues are identified early in the system's development lifecycle.

Smart grids

Smart grids, as part of an electricity power system, can intelligently integrate the actions of all users connected to it - generators, consumers and those that do both - in order to efficiently deliver sustainable, economic and secure electricity supplies.

Smart meter

In addition to traditional metering functionality (measuring and registering the amount of energy which passes through it), smart meters are capable of two-way communication allowing them to transmit meter reads and receive data remotely.

Smart metering regulatory regime

The regime which will provide the arrangements for the introduction and ongoing operation of smart metering. These regulatory arrangements will be introduced using powers under the Energy Act 2008 to amend existing licences and codes, and to create a new licensable activity and a new licence.

T

Technical interoperability

The capability of systems or devices to provide and receive services and information between each other, and to use these services and information exchange to operate effectively together in predictable ways without significant user intervention. Within the context of the smart metering system, this means the seamless, end-to-end connectivity of hardware and software from customer premises equipment through to DCC, suppliers, network operators and other authorised parties.

Technical specifications

The technical specifications for the smart metering system will be an explicit set of solutions and guidelines as to how the smart metering system will fulfil the functional requirements.

Time-of-use tariff

Under a time-of-use tariff, a supplier varies its charges based on when energy is used (e.g. day/night; peak/off-peak; or by season). Such tariffs can be dynamic (changes in real time) or static (changes at predictable times).

W

Wide area network (WAN)

The smart metering WAN will be used for two-way communication between smart meters and DCC (via the WAN communications module in the customer's premises).

Appendix 4 – The Authority's Powers and Duties

1.1. Ofgem is the Office of Gas and Electricity Markets which supports the Gas and Electricity Markets Authority ("the Authority"), the regulator of the gas and electricity industries in Great Britain. This Appendix summarises the primary powers and duties of the Authority. It is not comprehensive and is not a substitute to reference to the relevant legal instruments (including, but not limited to, those referred to below).

1.2. The Authority's powers and duties are largely provided for in statute, principally the Gas Act 1986, the Electricity Act 1989, the Utilities Act 2000, the Competition Act 1998, the Enterprise Act 2002 and the Energy Act 2004, as well as arising from directly effective European Community legislation. References to the Gas Act and the Electricity Act in this Appendix are to Part 1 of each of those Acts.[10]

1.3. Duties and functions relating to gas are set out in the Gas Act and those relating to electricity are set out in the Electricity Act. This Appendix must be read accordingly[11].

1.4. The Authority's principal objective when carrying out certain of its functions under each of the Gas Act and the Electricity Act is to protect the interests of existing and future consumers, wherever appropriate by promoting effective competition between persons engaged in, or in commercial activities connected with, the shipping, transportation or supply of gas conveyed through pipes, and the generation, transmission, distribution or supply of electricity or the provision or use of electricity interconnectors.

1.5. The Authority must when carrying out those functions have regard to:

- the need to secure that, so far as it is economical to meet them, all reasonable demands in Great Britain for gas conveyed through pipes are met;
- the need to secure that all reasonable demands for electricity are met;
- the need to secure that licence holders are able to finance the activities which are the subject of obligations on them[12];
- the need to contribute to the achievement of sustainable development; and
- the interests of individuals who are disabled or chronically sick, of pensionable age, with low incomes, or residing in rural areas.[13]

1.6. Subject to the above, the Authority is required to carry out the functions referred to in the manner which it considers is best calculated to:

[10] Entitled "Gas Supply" and "Electricity Supply" respectively.
[11] However, in exercising a function under the Electricity Act the Authority may have regard to the interests of consumers in relation to gas conveyed through pipes and vice versa in the case of it exercising a function under the Gas Act.
[12] Under the Gas Act and the Utilities Act, in the case of Gas Act functions, or the Electricity Act, the Utilities Act and certain parts of the Energy Act in the case of Electricity Act functions.
[13] The Authority may have regard to other descriptions of consumers.

- promote efficiency and economy on the part of those licensed[14] under the relevant Act and the efficient use of gas conveyed through pipes and electricity conveyed by distribution systems or transmission systems;
- protect the public from dangers arising from the conveyance of gas through pipes or the use of gas conveyed through pipes and from the generation, transmission, distribution or supply of electricity; and
- secure a diverse and viable long-term energy supply.

1.7. In carrying out the functions referred to, the Authority must also have regard, to:

- the effect on the environment of activities connected with the conveyance of gas through pipes or with the generation, transmission, distribution or supply of electricity;
- the principles under which regulatory activities should be transparent, accountable, proportionate, consistent and targeted only at cases in which action is needed and any other principles that appear to it to represent the best regulatory practice; and
- certain statutory guidance on social and environmental matters issued by the Secretary of State.

1.8. The Authority has powers under the Competition Act to investigate suspected anti-competitive activity and take action for breaches of the prohibitions in the legislation in respect of the gas and electricity sectors in Great Britain and is a designated National Competition Authority under the EC Modernisation Regulation[15] and therefore part of the European Competition Network. The Authority also has concurrent powers with the Office of Fair Trading in respect of market investigation references to the Competition Commission.

[14] Or persons authorised by exemptions to carry on any activity.
[15] Council Regulation (EC) 1/2003