



## Detica Response to Ofgem's Smart Metering Prospectus September 2010

© 2010 Detica Limited – a BAE Systems Company. All rights reserved

### **Confidentiality**

All information contained in this document is provided in confidence for the sole purpose of adjudication of the document, and shall not be published or disclosed wholly or in part to any other party without Detica's prior permission in writing, and shall be held in safe custody. These obligations shall not apply to information that is published or becomes known legitimately from some source other than Detica.

## Table of Contents

<b>1.</b>	<b>Executive Summary .....</b>	<b>3</b>
1.1.	About Detica.....	3
1.2.	Our collaboration with BT and Arqiva.....	3
1.3.	The structure of this document .....	3
1.4.	Summary of our observations and recommendations .....	4
1.5.	Contacting us.....	6
<b>2.</b>	<b>Securing smart meters .....</b>	<b>7</b>
2.1.	Recommended key overarching principles.....	7
2.2.	Governance of Security and Privacy.....	8
2.3.	Understanding the security and privacy risks .....	10
2.4.	The specification of the security solution .....	11
2.5.	The security challenges of the staged implementation.....	14
<b>3.</b>	<b>Our responses to Prospectus questions .....</b>	<b>16</b>
3.1.	Prospectus .....	16
3.2.	Communications Business Model.....	30
3.3.	Consumer protection.....	32
3.4.	Data Privacy and Security.....	34
3.5.	Implementation Strategy .....	37
3.6.	In-home Display .....	45
3.7.	Non-domestic Sector .....	49
3.8.	Regulatory and Commercial Framework .....	50
3.9.	Rollout Strategy .....	53
3.10.	Statement of Design Requirements .....	59

# 1. Executive Summary

## 1.1. About Detica

Detica is a specialist in delivering complex information management and security solutions to a range of government, Critical National Infrastructure and commercial clients. We are a subsidiary of BAE Systems plc, the premier global defence, security and aerospace company and therefore are able to provide a broad range of leading edge technology and security solutions, as well as the ability to effect the type of complex national change that the Smart Metering programme will entail.

## 1.2. Our collaboration with BT and Arqiva

The successful implementation of smart meters and the smart grid in Great Britain will be dependent on a robust and secure infrastructure which provides connectivity, data management and shared industry processes. This is a complex undertaking which will require a number of best of breed service providers to work together to design, build and operate a solution that will endure for the lifetime of the meters.

In July 2010, British Telecom (BT), Arqiva and Detica announced a collaboration<sup>1</sup> to offer a universal, dedicated, secure and resilient nationwide communications network to underpin the Government's plans for smart meters and subsequent smart grid applications. This group brings together significant expertise in delivery of nationwide communications systems as well as leading edge security capability.

We have consulted widely across the industry in preparing our response to the Prospectus, and have shared our views openly with a view to building consensus among stakeholders so that the optimal solution is delivered, and is right first time.

## 1.3. The structure of this document

This document contains Detica's comments on the Prospectus together with answers to the specific questions posed. In order to provide a complete and balanced response, we have collaborated closely with BT and Arqiva as well as many other stakeholders of the programme.

Detica's comments are structured as follows:

- **Section 1** (this section) – Detica's summarised recommendations, coverage of our key observations and comments on the issued Prospectus documents;
- **Section 2** – A summary of Detica's views on how to secure smart meters optimally, both in terms of cost effectiveness and in safeguarding the achievement of the programme's benefits;
- **Section 3** – Our responses to specific questions raised in each section of the Prospectus. These responses echo those of our collaboration partners, BT and Arqiva. We recognise the need for timely feedback, and so this section contains our response to questions with a 28<sup>th</sup> September deadline, as well as initial responses to questions with a 28<sup>th</sup> October deadline. We may provide an update for the October questions in due course to reflect any material updates in the coming month.

---

<sup>1</sup> Please refer to <http://www.detica.com/about-us/news-and-events/press-releases.html?id=1&task=asset&Artid=652>

## 1.4. Summary of our observations and recommendations

We welcome the clarity that the Prospectus brings to some very complex issues and the significant amount of analysis and consultation that has been required to bring it to this stage. We understand that rolling out 47 million meters, whilst minimising costs and maintaining competition in the market, is a highly complex undertaking and that further work is required to reach an agreed specification and design. We therefore offer the following suggestions to support this endeavour.

### Key Challenges

We share the sense of urgency that is building around the implementation of smart meters and smart grids in Great Britain. The procurement of an interim solution from 2012, however, has significant commercial and technical challenges, and as such will not support a rollout at scale prior to the establishment of the Data Comms Company (DCC). As such, we believe that the approach outlined by Ofgem is unlikely to deliver the programme objectives by 2020:

1. Procuring the interim solution on a piecemeal basis will bias the market towards mobile (GPRS) communications, and may then make switching to a more suitable, future proof solution uneconomic<sup>2</sup>. The alternative of maintaining the interim solutions alongside the enduring communications solution will increase communications costs by £360m, not including additional systems integration costs associated with duplicate solutions;
2. Assuring the security of the interim solution will be difficult without a central body to oversee and manage security operations. Rolling out an interim solution without a robust and coordinated security solution will increase the likelihood of a security incident in the interim period. This is likely to greatly undermine public confidence in the programme and has the potential for significant consequential loss (for example due to interrupted power supply);
3. Following the appointment of the DCC the timescales for subsequent procurement of service providers and the building and testing of a national solution are, in our opinion, unlikely to be achievable as the current time allocated to deliver these activities are too aggressive. In the event of slippage, a continuation of scale rollout would increase the stranding costs associated with the interim solution and could make the procurement of a more suitable enduring solution uneconomic. This would undermine the programme benefits case and could raise the prospect of a legal challenge;
4. The transition from the interim solution to the enduring DCC-led solution may be problematic. Unless they are developed under the governance of an overall solution design authority, "early mover" solutions will not be based upon an agreed and interoperable set of requirements and specifications. When the DCC is established, this mixture of technologies would either need to be replaced (costly) in order to deliver to national service standards, or to be retained (thereby leading to different service quality standards);
5. The DCC will not have the resources, skills and experience to procure and integrate a national scale integration successfully. Procurement and delivery of a national smart metering solution is a significant and complex undertaking. Given that the DCC will be a new entity, it is most unlikely to have these integration skills on its appointment and there are a number of examples in the public domain where public sector agencies have struggled with the integration challenge. With appropriate contractual preparation (such as the setting of a requirements baseline) and fair risk/reward mechanisms, a consortium from the private sector is better placed to meet this challenge.

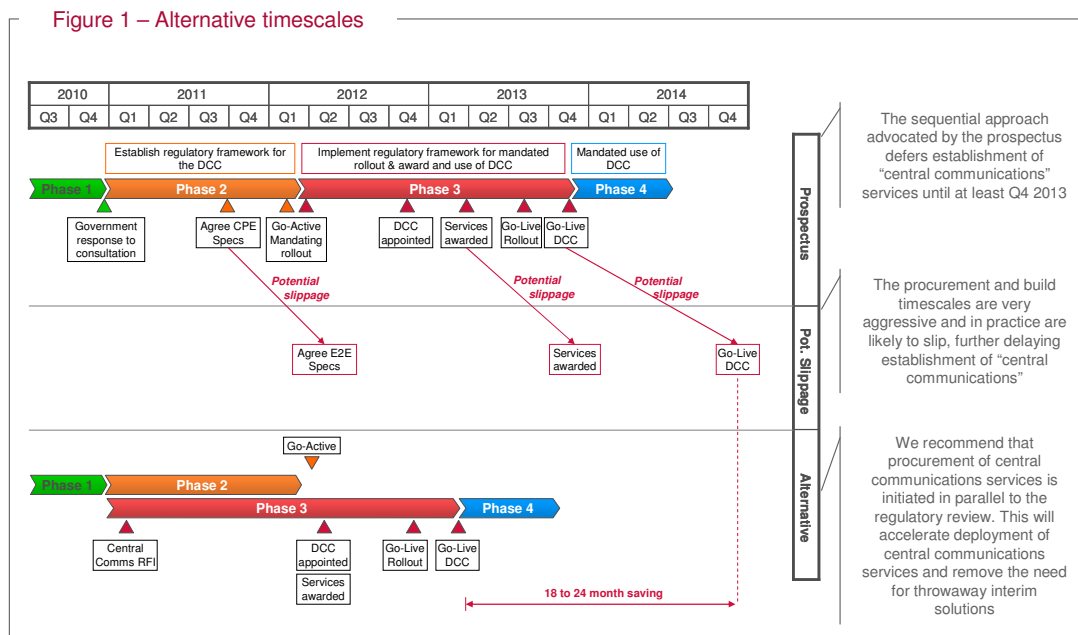
---

<sup>2</sup> We estimate the cost of replacing the "interim" WAN communications modules to be in excess of £580m

### Key recommendations

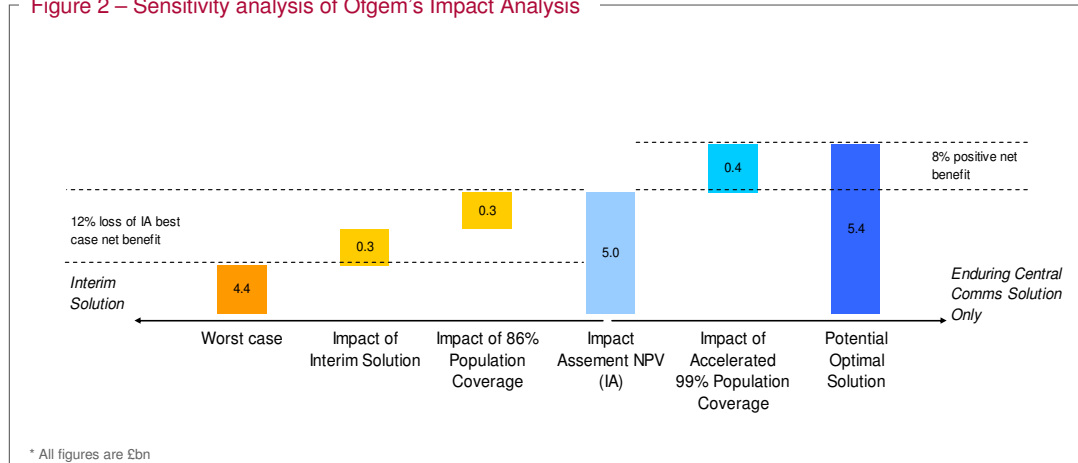
1. Early procurement (from Spring 2012) of a limited set of DCC service providers, run in parallel to the definition of the regulatory framework. We recommend that procurement of a national communications and security provider is initiated in 2011 with a view to making this service available to all stakeholders from 2012;
2. Continue the appointment of the DCC as code administrator. The national communications service may then be transferred across to this body as envisaged by the Prospectus;
3. No mandated supplier rollout from 2012. Mandate rollout from suppliers only once the national communications infrastructure and associated standards have been established;
4. Competitively procure national communications, security and data services from a consortium with end-to-end accountability for delivery. This approach will provide greater certainty of delivery and will minimise delivery risk, as well as providing clear accountability for service provision.

This approach is illustrated in Figure 1 below.



Detica, BT and Arqiva have carried out a sensitivity analysis (see Figure 2 below) of Ofgem's Impact Analysis. This sensitivity analysis evaluates the financial impacts of some of the challenges we have identified, as well as the incremental benefits associated with our recommendations.

Figure 2 – Sensitivity analysis of Ofgem's Impact Analysis



Potential NPV downsides associated with the interim solution:

- £0.3bn net loss is from having a 2 year interim solution and then swapping out all interim in home communications modules for the strategic solution;
- £0.3bn net loss is from using a GPRS solution with limited to coverage and a 6 year accelerated meter rollout in comparison to the base meter rollout case (adjusted to 99% coverage) as outlined in the Prospectus.

Potential NPV upsides associated with an immediate adoption of an enduring, universal solution:

- £0.4bn net benefit is from using a solution (such as Long Range Radio) that provides 99% coverage in 2 years and rolling out meters over an accelerated 6 year period in comparison to the base meter rollout case (adjusted to 99% coverage) as outlined in the Prospectus.

Further significant, but currently un-quantified, benefits will accrue from a shared security managed service. These un-quantified benefits will be modelled when an agreed view of the risk landscape is available.

## 1.5. Contacting us

To discuss any of the contents of this document or Detica's services, please contact:

Ian Watts  
 email: [ian.watts@detica.com](mailto:ian.watts@detica.com)  
 Telephone: 01483 816 095

## 2. Securing smart meters

### 2.1. Recommended key overarching principles

Delivering a national communications infrastructure is complex and expensive and so care is needed to ensure that the right solution is adopted, and costly rework avoided. Based on our own experience, as well as extensive consultations with energy suppliers and Distribution Network Operators (DNOs), we believe that the following overarching design principles need to be adopted, and have therefore based our recommendations and feedback on them.

- i. **Provide a stable basis for industry to innovate in technology and product offerings**
  - Smart meters are an important stepping stone towards the establishment of smart grids. For this to be the case, however, the coverage, capacity, resilience and latency of communications, data and security solutions must be specified to support both metering and smart grid applications;
  - Delivering smart grid capability will involve considerable capital expenditure and integrating these solutions with communications modules is not trivial. Any solution adopted must have a designed life equivalent to the network hardware and metering assets that they support (i.e. 15 years).
- ii. **Best consumer experience possible**
  - Consumer support is vital to the success of the programme, not least as one of the most expensive parts of it is the need to visit each household to change meters. The inconvenience of waiting at home for an engineer to arrive to install meters will be a major annoyance. This will be exacerbated for those customers who purchase their electricity and gas from different suppliers. Consideration should therefore be given to removing the interdependency between suppliers by allowing for a communications card (from each supplier) in each meter;
- iii. **Protect the security of individuals and the nation and safeguard individual's privacy**
  - Modern society is reliant on a safe and secure supply of energy. Smart meters will form a fundamental part of the Critical National Infrastructure, upon which all other industries rely. Robust security standards and built-in resilience must be adopted to reduce the threat of subversion of the network, or errors by its operators and users, along with active monitoring and review to anticipate, detect and respond to new threats;
  - An individual's security and privacy must be safeguarded to protect them from intrusive marketing, theft and fraud, as well as accidental loss of data. The solution must be capable of helping the consumer to manage who has access to their data, as well as providing back up in the event personal data or prepay credit is lost – but without placing unrealistic expectations on them.
- iv. **Maximise the value of the solution**
  - The smart metering programme is a significant undertaking involving an investment in excess of £10bn. Ofgem's Impact Analysis anticipates that over 21 years it will deliver a Net Present Value of £5bn. Careful planning of the solution and delivery approach will be needed to achieve or exceed this figure;
  - Minimise Total Cost of Ownership (TCO), by selecting a solution that minimises installation costs, which provides an enduring solution and allows for easy asset and service transfer;
  - Minimise delivery risks by ensuring that a prime contractor has the responsibility and capability to deliver a turn-key solution;

- Maximise the speed of rollout by selecting an enduring communications service from the start that does not constrain the pace at which meter installations can be carried out whilst also being demonstrably secure.
- v. **Universal standards of coverage and service**
- Coverage - The Prospectus calls for smart meters to be installed in every home in Great Britain. Achieving that will require a communications solution with 100% coverage;
  - Availability – The end to end smart metering system must have the ability to continue to operate under diverse operating conditions, including but not limited to peak load conditions, attacks, maintenance operations, and normal operating conditions;
  - Latency – The communications infrastructure will form the basis of GB's smart grid infrastructure, and so needs to operate at a latency that is acceptable to Distribution Network Operators (DNOs). Taking into consideration emerging smart grid requirements, the Prospectus calls for near-real time data transfer to support planning and active load management. Our discussions with the industry have suggested that requirements for ultra-low latency (real time) data transfer for load management will be a prerequisite.

## 2.2. Governance of Security and Privacy

The deregulated energy industry in Great Britain is complex. It delivers many important benefits to the consumer in terms of choice and pricing and is viewed as one of the most competitive energy markets in the world. However, a highly competitive energy market, with a diverse range of government, commercial and individual stakeholders, inevitably further complicates the security challenges with smart metering.

Delivery of smart meters and a smart grid will require a range of businesses to co-operate to deliver elements of the solution. The interconnected nature of this infrastructure between different organisations will mean that no single industry body can have overall control over the ecosystem, although all are potentially impacted by cyber attacks.

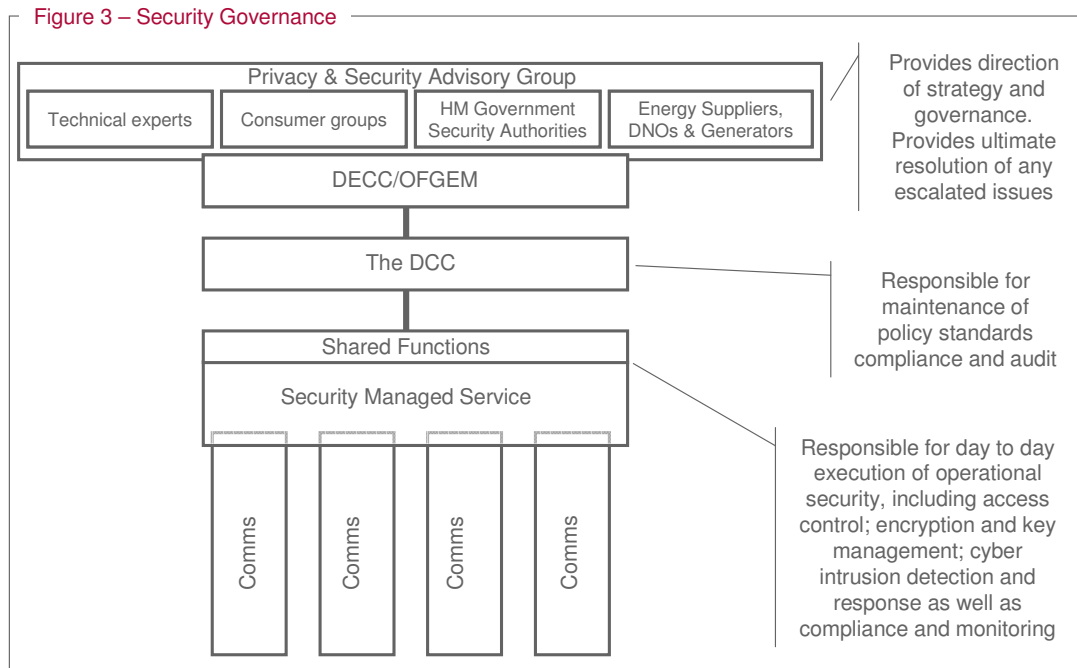
In our white paper "*Securing Smart Meters: getting it right first time*"<sup>3</sup> we highlighted the need for separate bodies to manage the review and development of security strategy, industry governance, and management of operations and response to any incidents that arise.

We envisage that the development and maintenance of the security strategy and governance arrangements will ultimately remain the responsibility of DECC and Ofgem, advised by a panel of interested parties, including government security authorities, industry representatives, as well as technical experts and appropriate consumer groups.

The DCC, as code administrator, should, in our view, be responsible for applying governance over the industry, through a set of agreed policies and standards, and would ensure that these are regularly and independently audited.

---

<sup>3</sup> For a copy of this white paper, please visit <http://www.detica.com/about-us/insights.html?task=assetdownload&Artid=497>



The DCC will need to procure a specialist service provider to provide a managed service to execute the operational security management service. In practice it will be difficult to separate this service from the provision of WAN communications and shared functions such as registration due to their interconnected nature.

This “Security Managed Service” should include the following capabilities:

- **Access control**

Access control is in essence the implementation of security governance, and will include a range of components such as a request validation system, rights management, authentication, enhanced authorisation, certificate management with threat control, to ensure secure and valid access to the meters as well as internally within the DCC.

Access control also includes: Secure access to meters, to the internal DCC infrastructure, as well as secure routing of meter data and other HAN messages to a multitude of authenticated industry end-points / back-office systems.

A centralised access control layer forms the gateway and the first line of defence for the smart metering landscape as well as any DCC. It needs to be bi-directional to ensure that the industry has specific and role-based access to meter data while assuring that scheduled reads, alarms, configuration and firmware updates and real-time messages are sent to a valid, authenticated end-point.

- **Permissions management**

Detica believes that a roles-based access control must be implemented in order to secure the DCC and ensure the principle of least access to the data. This must include an identity management solution controlling authentication and authorisation of any user access request for the entire solution. Such a solution also provides centralised identity management for internal and external users of the solution, implementing roles and responsibilities for associated identities driving authorisation.

- **Encryption and key management**

A centralised system to manage encryption keys and certificates for all systems in the solution will be required before the start of any mandated rollout to ensure secure

communication of meter and event data. This need is further increased by the requirement to deliver a centralised Prepayment System.

Detica believes that individual key management systems, hosted individually by meters or suppliers would create proprietary metering systems and integration issues. Currently meters are encrypted by manufacturers and public keys, rather than certificates that bind the key to a particular meter are distributed to back-office systems. At present a change of supplier could necessitate exchange of keys between suppliers and storage of new keys in meters leading to technical and operational challenges.

- **Intrusion detection and response**

The capability for cyber-intrusion prevention and detection must be implemented to ensure that the industry interfaces to and from the DCC (and across the meter population) are free from known intrusion and disruptive network traffic. It furthermore needs to provide protection of the IT perimeter of the DCC. Intrusion detection includes data collection and monitoring, detection, investigation, response and proactive improvement.

### 2.3. Understanding the security and privacy risks

Securing a complex information and communications technology solution is always a balance between the level of assurance provided and the costs of the assurance. As such it is a matter of risk reduction to a level considered tolerable and affordable, rather than complete avoidance of all risks. The first step of this is the completion of an end-to-end risk assessment.

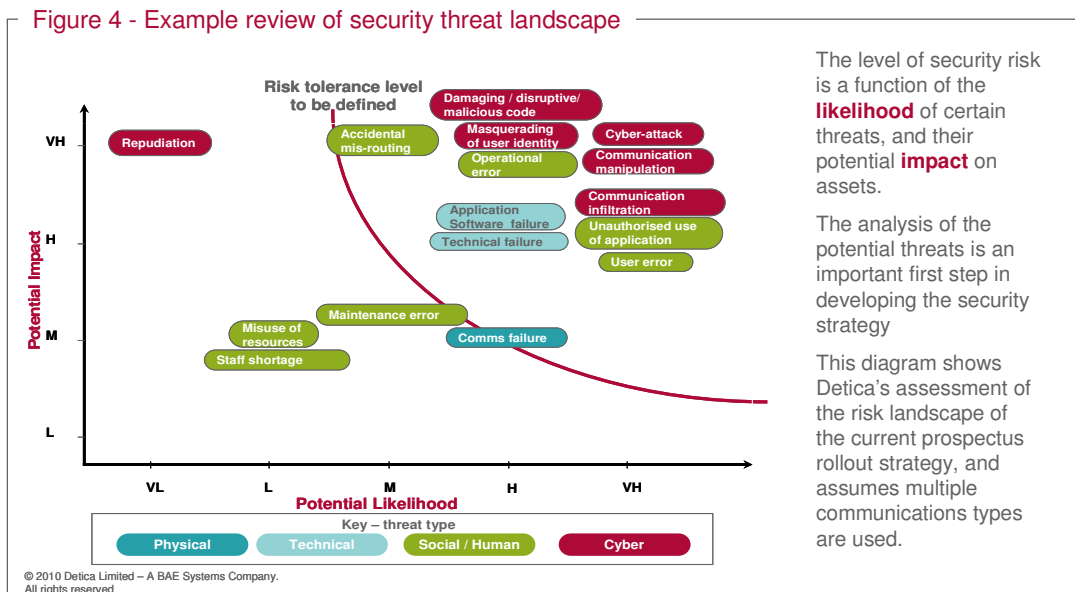


Figure 4 illustrates this principle, and shows a matrix which gives examples of risks plotted by their impact and likelihood. Smart metering will introduce a new dimension of risks which need to be understood before appropriate responses are designed. The nature of these risks is influenced by a range of factors such as the specification of the meters, the communications business model, as well as the types of technologies used.

Detica is pleased to observe that Ofgem has understood the need for this risk assessment, and has started to create a risk assessment using Her Majesty Government's (HMG) Secure Policy Framework (SPF) and its underpinning risk tools (albeit that no outputs have so far been shared with the industry). We would, however, note that this is a complex risk management tool designed for government to ensure confidentiality rather than security,

which relies heavily on technical risk assessments and restrictive standards. This approach could restrict market entry into the sector for smaller parties who may not understand this methodology or have the ability to gain access to the relevant highly complex documentation. The risk assessment must also consider integrity and availability and drive out requirements for procedural and personnel controls.

As this may not be the optimal approach for a Critical National Infrastructure programme such as this, where integrity and availability are *at least as* important, we would recommend a holistic approach that draws the best elements from a range of methodologies<sup>4</sup> but which is aligned with the ISO27000 series of information security standards. This will allow the market to choose whatever methods suits them best, and allow for innovation and enablement of the programme. We also highly recommend that any prospective supplier to the programme be ISO27001 certified to allow for a common comparability and credibility baseline.

As part of our Security Horizons<sup>5</sup> programme, Detica has carried out an independent review of the smart metering risk landscape based on extensive consultation across energy, communications, government and other stakeholder groups, and have developed a consensus view that we have previously shared with Ofgem.

## 2.4. The specification of the security solution

### Guiding principles for the security and privacy solution

Based on the vision for smart metering and our initial understanding of the risk landscape, we recommend that the following overarching design principles are adopted for the services provided under the DCC's remit:

- i. **Regarded as Critical National Infrastructure, with commensurate security and resilience standards**
  - DCC is dynamically engaged with security authorities (CPNI, CCS, CESA, etc)
  - DCC forms a key part of the CPNI's Energy IE (Information Exchange)
  - Incorporates crisis management capability
  - Service continuity management including data recovery capability
  - Resilience commensurate with CNII as well as utilities requirements
  - Continued availability of meter / end-point data
- ii. **Demonstrable compliance to industry regulation and international standards**
  - ISO270001 / BS25999 certified
  - Freedom of Information and Data Protection Act compliant
  - Ofgem and Ofcom governed
  - Ensures appropriate implementation of Privacy Enhancing Technologies (PETs)
- iii. **Demonstrable system and service integrity**
  - Forensic readiness - auditable and audited
  - Continuous event logging and tracking
  - Includes fraud management capability
  - Transactional integrity (authentication)
  - Effective archiving / retention policies implemented
- iv. **Addresses the cyber security challenge**
  - The proposed solution has the ability to detect unusual behaviour consistent with organised crime or malicious attacks
  - Includes active (24x7) cyber intrusion management

<sup>4</sup> such as CRAMM, IRM, NIST and ISF (FIRM,SARA,SPRINT,IRAM)

<sup>5</sup> Detica's Security Horizons programme is a co-ordinated series of discussion events and thought-provoking research - [www.detica.com/securityhorizons](http://www.detica.com/securityhorizons)

- v. **Incorporates “strong” identity and access management controls**
  - Incorporates rigorous role management
  - Includes strong access control and authorisation
  - 3 factor Authentication implemented on key roles and to key processes
- vi. **Assured behaviour of staff and organisations**
  - Strong consideration of human factors
  - Focus on security awareness, education and training
  - Includes vetting of delivery staff
  - Incorporates validation of organisational credentials
- vii. **Strong disclosure and sharing control**
  - Disclosure of data governed by rights management
  - Registered information sharing implemented
- viii. **Designed for growth and enables expansion**
  - The solution has the ability to support infrastructure life of 15 years or more
  - Provides for inclusion of smart grid functionality, water as well as micro-generation and electric vehicles

**Controls and standards**

The selection of actual controls needs to be driven by both the overarching principles and by the risk assessment. Based on the analysis already completed by Detica, we would advise a comprehensive set of controls in recognition of the Programme’s importance to the Critical National Infrastructure, that ensure that known and anticipated risks are appropriately managed.

The strength of these security controls must be commensurate with the potential impact and likelihood of the risks faced. The level of assurance provided by these controls must be balanced by the Industry Advisory Group to reduce the risk as far as possible as it is important to recognise that no one is in a position to guarantee that any Information and Communications Technology (ICT) solution is 100% secure against all current and future threats. Detica is therefore using our “Security Horizons” discussion forum to prompt constructive debate about these trade offs. Figure 5 illustrates this principle:

Figure 5 – Illustration of cost/assurance trade off when designing controls

Sample Controls & Capabilities	Strength of Control			The strength of controls is determined by the level of risk identified by the risk assessment (see Figure 3)  These will be a trade off between the level of assurance provided and the cost of implementing them  The blue shaded cells illustrate that these trade offs are made on a case by case basis for each control type
	High assurance / Higher Cost		Low assurance / Lower Cost	
Hardware Controls	E.g.: Near line, offline plus off-site tape storage	E.g.: Off-line plus off-site	E.g.: Off-line; Reactive	
Software Controls	E.g.: Identification using smart cards and certificates;3 Factor Authentication	E.g.: Identification based on user ID-2 Factor Authentication;	E.g.: Gatekeeper only; User ID / Password	
Communication Controls	E.g.: High-grade Crypto; Traffic padding; IDS at every entry point	E.g.: Commercial crypto; IDS at entry points	E.g.: Hashed Checksum only IDS at internet facing only	
Procedural Controls	E.g.: Unit test after each check-in Rigorous application of standards and patterns	E.g.: Unit test at pre-determined intervals Best practise development	E.g.: Loosely adhering to standards and patterns	
Personnel Controls	E.g.: All staff Security Cleared to SC level	E.g.: Granular clearance based on role	E.g.: Security Clearance for known problem areas only	
Physical Controls	E.g.: Extensive Perimeter Security	E.g.: Secure Facility	E.g.: Commercial Facility with adequate Security	

A comprehensive set of security controls is required to ensure that known and anticipated risks are appropriately managed, and these will include:

- **Implementation of a consent framework**  
Required to address the full issues of gaining consent from the consumer that extends the boundaries of the Data Protection Act to allow for informed active consent rather than the typical "presumed consent" and "opting out".
- **Centralised access brokering**  
A centralised access control and authorisation brokering system should be delivered early in the programme to ensure security interoperability and consumer protection. Also agreement needs to be reached on role based access control and authentication and encryption for the sensitive processes within the smart metering system.
- **Encryption standards**  
A fully federated key management and encryption service, (the use of asymmetric techniques for distribution of symmetric keys), will be required to provide the necessary protection for sensitive meter data. We believe that a dedicated and centralised encryption management system will be able to provide a fully federated encryption service and allow independent route selection for data transfer.
- **Vetting**  
The threat to security from insiders is a reality especially during turbulent times; Standards must include the appropriate level of clearance required to work on the smart metering system, and to perform critical roles within it.
- **Training and competence**  
The smart metering system, managers administrators and processors users must have the correct training and competence to carry out tasks on the system without making a mistake that could effect the security of the system. All users need to be accountable for the task required of them, and this cannot be enforced without the proper training, competence checking and enforcement regimes.
- **Communication standards**  
Standards must be established for communication protocols and ports to be used. This will enable gateways and firewalls to control these communications and unnecessary services on servers et cetera, to be switched off reducing the scope for attacks and potential for information leakage.
- **Physical security standards**  
Agreement needs to be reached on which physical standards the smart metering system needs to comply with; eg CPNI Policy and best practice would need to be made available to all suppliers or use:
  - BS 8220-2:1995 Guide for security of buildings against crime. Offices and shops
  - BS 8220-3:2004 Guide for security of buildings against crime. Storage, industrial and distribution premises.
- **Alarm management by the DCC**  
Security standards must be defined and implemented for alarm management. Agreements indicating the event's severity, and the actions required must be outlined to enable stakeholders to have a common understanding of the reason for the alarm and thereby respond appropriately and efficiently to minimise the duration, impact and cost of any events.
- **Transaction approval**  
All transactions across the landscape need to be authorised to enable the protection of the consumer and the availability of the smart metering system as a whole.
- **Application development standards**  
Applications need to protect data from unauthorized access or modification and ensure its availability "by design". During the last few years, the number of vulnerabilities being

discovered in applications is far greater than the number of vulnerabilities discovered in operating systems. As a result, more exploitation attempts are recorded on application programs. Applications will therefore need to be subject to robust vulnerability assessment and penetration testing before go-live as well as in-life.

- **System operations:**  
All systems in the end-to-end infrastructure must be supported by clear and rigorous operating procedures that include security operating procedures.
- **Information security certification**  
All suppliers and service providers of smart metering systems need a common platform to start from. Formal certifications should, therefore be required to ISO:27001 (Information security) and BS25999 (Business Continuity<sup>6</sup>).
- **Crisis management**  
A crisis management capability is needed to enable the system to recover itself as a whole rather than individual parts, whilst providing a continuous minimum service throughout.
- **Governance framework**  
A Governance framework is required to oversee the standards and procedures under which the smart meter system functions can be governed. The smart metering system needs a strong security policy framework in place that is agreed by all.
- **Intrusion management**  
Threats to the smart metering system range between external, internal and passive. The smart metering system must be adaptable to the changing complexity of the threat landscape and be able to provide protection for a wide variety of new viruses' trojans, worms or mobile code attacks that may be presented by remote end points. Intrusion management systems are vitally important to network security. With attacks originating inside as well as outside, a multi provision intrusion management approach is an essential element of defence.
- **Code of connection**  
Compliance standards will be required for the security posture and practices of all parties connecting to the DCC. A compliance auditing process will be required to give assurance to the Privacy and Security Advisory Board and thence the governance board as well as all connecting parties.
- **Auditing and monitoring**  
Conventional audit and monitoring may be insufficient to detect low-level network attacks. Many audit trails generate irrelevant or insufficient information for monitoring stations and many incidents go un-noticed until too late and ultimately may only surface under a forensic investigation into the causes of a major incident. A proactive Cyber Intrusion Management solution is therefore needed.

## 2.5. The security challenges of the staged implementation

We welcome the ambition to accelerate the deployment of smart meters, however the staged implementation approach will introduce significant additional security risks. In this scenario, each of the energy suppliers would be responsible for building their own solutions, albeit against some common standards, with a view to migrating these solutions to the DCC once it is established.

The early phases of smart meter rollout will be subject to considerable public scrutiny, and any major security incident will undermine public confidence. It is prudent to expect that the

---

<sup>6</sup> When available in the near future

appetite of individuals or groups for subverting the system will be higher due to the greater likelihood of publicity and the likelihood that the control regime is immature. We would, therefore strongly recommend that careful consideration is given to the security considerations of the proposed staged implementation approach, in consultation with the relevant authorities.

Protecting the security and privacy of the meters under this scenario will be problematic for the following reasons:

- Controlling access to data from multiple different legacy solutions<sup>7</sup> will be cumbersome and inefficient. Suppliers will implement access control using differing technologies at various levels and with varying rigour within their systems' portfolio. This will then be highly problematic when consumers change suppliers, or wish another entity to be able to view their data. To enable interoperability, a central federated access control and authorisation service needs to be provided.
- Centralised key management is needed to ensure that encryption of communications can be efficiently managed. – To prevent interception and subversion of data, it needs to be encrypted from the meter, through to the DCC. Relying on point-to-point encryption provided by existing communications technologies will not be effective<sup>8</sup>. A solution which allows regular refresh of encryption keys is therefore needed. It will not be practicable to manage such a solution in a decentralised way. Localised encryption keys then being redirected to the DCC will also be impractical, thereby potentially making the change of supplier process even more complex.
- Intrusion detection capability is likely to be piecemeal and ineffective – Each energy supplier would be responsible in the interim for their own intrusion detection, including managing the “Advanced Persistent Threat”<sup>9</sup> which they and their information and communications technology suppliers will be ill-equipped to do. This will be a short term solution to them, so they are unlikely to invest significantly in new capabilities to detect the early signs of cyber intrusion. Furthermore, a determined intrusion attempt will take place over a range of different parts of the solution (e.g. interception of communications signals, spoofed identities to circumvent access controls, rogue insiders), and may be undetectable to individual suppliers. Adequate assurance and optimal operational response can, therefore, only be provided by a shared security management service with oversight of all components. If this is not provided, in addition to suppliers own capabilities and in the light of Her Majesty Government's own Cyber Security Operations Centre (CSOC) needing a single point of contact, DECC and Ofgem would still need to establish a (sub-optimal) coordination centre to liaise with all suppliers.
- A coordinated response is required for coordinated attacks – Where a major intrusion is detected this is likely to affect multiple suppliers and multiple parts of the smart metering solution. A coordinated body is required to analyse the source and nature of the threats, as well as to oversee the execution of the response strategy and any updating of the controls. DECC and Ofgem are unlikely to have the capability to achieve this.
- Building a suitably robust and resilient security capability, bespoke to smart metering, within each supplier, will be duplicative and expensive, especially if it is to then be transitioned to a new service provider in the short term – energy suppliers do not currently face a significant cyber threat, and therefore their organisational capability to deal with it will require significant investment. Acquiring and operating technologies such as access control, encryption and advanced intrusion detection and response are specialist areas and it will be both more economic and effective to procure these as a shared service.

<sup>7</sup> I.e. the “interim” solutions implemented by each Supplier during the mandated staged roll out

<sup>8</sup> There are already well known methods of decrypting existing communications signals, and it is likely that methods will be quickly developed to decrypt new communications

<sup>9</sup> Advanced Persistent Threat is HM Government terminology for a technologically advanced cyber intrusion by state sponsored or organised crime bodies to obtain information of value, as well as simply embarrass the attacked body

### 3. Our responses to Prospectus questions

#### 3.1. Prospectus

<b>Q1</b>	<i>Do you have any comments on the proposed minimum functional requirements and arrangements for provision of the in-home display device?</i>
<p>The in-home display (IHD) has two purposes:</p> <ul style="list-style-type: none"> <li>To enable consumers to interact with some basic functionality of the meter (e.g. pre-payment top-up and gas or electricity reconnection acknowledgement)</li> <li>To display information about a consumer's energy (and in the future water) usage.</li> </ul> <p>The first of these will be required where consumers will not be able to easily access the meter itself, and as such should be included in the minimum functionality.</p> <p>The second is to support consumers in changing their energy usage behaviour by providing feedback (to them). To this end there is a greater range of functionality that can be considered. However, this additional functionality will increase the cost of devices and therefore presents a trade-off between the costs of providing devices by the suppliers against the level of engagement of consumers to deliver the behavioural change necessary.</p> <p>Although the research evidence into the use of IHDs by consumers is mixed, there is some evidence that most consumers use the display for the first few months allowing them to reduce their energy usage and make savings. However, in the long run, many consumers stop using their devices and simply consign them to the cupboard drawer. In light of this rapid tail-off of usage of the IHD, we recommend that the IHD provided as part of the smart metering rollout should provide a very basic level of information display. The basic IHDs should have the following characteristics:</p> <ul style="list-style-type: none"> <li>The display needs to be portable if possible to allow for ease of locating in the home, so long battery life is important.</li> <li>The display needs to be easy to read and easily configurable to the consumer's needs and wishes, e.g. no point in showing gas consumption if the consumer does not have gas.</li> <li>The units that the consumer sees need to be easily changed to meet their needs, some will understand Kwh, but others may wish pence per minute/hour/day etc.</li> <li>Careful consideration needs to be given to how much information is displayed and how it is displayed to ensure its intelligibility. It is recommended that the Programme issue guidelines on this to ensure a minimum standard is provided on the "free" IHDs.</li> </ul> <p>However, smart meters should also provide open, secure interfaces to their data to allow a market in after-market IHDs and other devices (e.g. TV Set-Top boxes) that would let consumers who are dissatisfied with the base level of information provided but remain motivated to make behavioural change to "upgrade" their IHD. These external devices may also be able to use additional information from the Internet via a broadband connection to enhance the display. The types of additional functionality that the after-market devices might provide includes:</p> <ul style="list-style-type: none"> <li>Selection of a usage profile such that consumers can compare their profile day to day.</li> <li>Highlighting periods of cheaper electricity tariff. A traffic light system or use of different colours enable ease of notification to consumers may be effective.</li> <li>The presentation of carbon emissions could also be provided for more ecologically conscious consumers. However, it is acknowledged that the calculation of this information is far from straightforward.</li> </ul> <p>In conclusion the free IHD, which might have a short life, needs to be of low cost to maximise the initial benefits. The consumer can then decide how, and with what device, they will engage with for their on-going energy management. The open standard interface will ensure that there can be a number of providers who can compete in this space.</p>	

<b>Q2</b>	<i>Do you have any comments on our overall approach to data privacy?</i>
<i>"The customer shall choose in which way consumption data shall be used and by whom, with</i>	

*the exception of data required to fulfil regulatory duties”.*

We believe in principle that this is a positive step and will go some way in alleviating consumer concerns over data privacy. However, we also believe that there are a number of key points that would need further and careful consideration around data privacy:

- **Privacy by Design:** Data protection must be embedded within the core design of the system, should be introduced early and needs to be in place for the mandated rollout. In practice, therefore, this protection needs to be in place prior to the creation of the DCC in order to prevent experiences such as those which occurred in the Netherlands, which gave rise to concerns over privacy leading to its smart metering bill initially being rejected.
- **Consumer Consent:** Whilst we are in agreement that consumer consent for the collection, use and disclosure of meter data should be implemented, we believe that further consideration needs to be given to the requirements of consumers who may not be in a position to make informed decisions around what they are consenting to, and the level of consent that they have provided. Enforcement of consumer consent is also a cause for concern as the Data Protection Act, though holistic for personal data protection, may not be granular enough to cover specific meter data privacy. Further, serious consideration needs to be given as to how such consent management will be achieved where individuals are not 'digitally enabled' in an environment where meter and meter display functionality will be limited. We note that in the context of the Third Package Consultation by DECC (Consultation on the Implementation of the EU Third Internal Energy Package URN 10D/727 July 2010) that s105 of the Utilities Act as also considered relevant in relation to industry confidentiality requirements and would suggest that the effect of that section is also considered in the context of the development of the approach on data privacy.
- **Data Storage:** Mastering of data within the meters for a period of 12 months in theory provides greater control and ownership to the customers, however it also raises questions around data access and resilience:
  - A number of industry bodies require access to this data, not least the suppliers who would require regular and ad hoc access to data, albeit aggregated in order to make key customer and tariff management decisions.
  - Mastering data only within the meters will create a technological as well as process impracticability.
  - Singular data storage with no immediate back-up strategy will create resilience issues where meter data is lost by consumers (either wilfully or inadvertently).

The Programme should therefore give consideration to the possibility of a centralised data store, perhaps within the DCC. We would envisage the DCC working alongside the Information Commissioner's Office (ICO) to create specific meter data protection standards which might be included as part of the DCC licence.

- **Data Integrity and Confidentiality:** Storage of large amounts of data locally within the meters also introduces security concerns:
  - The ability to hack into, or interrogate meters, would allow for tampering or misrepresentation of meter data thus causing data integrity issues;
  - There is a further concern around sharing of meter data, for example through

rental turn-over or change of ownership of property. A change in tenancy status would mean new occupiers having access to meter data from previous incumbents. This could also cause a problem if residences change from domestic to non-domestic status, as this then raises questions over ownership of the data. Clearing down or sanitising this data without any other form of storage or data source would again cause loss of data, especially if the customer wishes their data to move with them.

**Q3** *Do you have any comments on the proposed approach to ensuring customers have a positive experience of the smart meter rollout (including the required code of practice on installation and preventing unwelcome sales activity and upfront charging)?*

We agree with the proposed approach. It is essential that the consumer experience is excellent, from early communications to completed installation, to build confidence in the new services. This is best achieved through a Code of Practice agreed by all suppliers and embedded within their modified licences. The Code will ensure that consumer communications, installation planning, installation visit (including installer identification, handling of difficult access, special provisions for elderly or disabled) and installation feedback are executed consistently and seamlessly, irrespective of supplier.

Installation visits should be only for physical works and consumer familiarisation, not sales - at least for the primary installation visit. If a subsequent visit is needed to fulfil a specific consumer driven order for higher value services (e.g. premium IHD, integration of micro generation products), then limited sales approaches could be included. The installer should be able to supply the consumer with collateral relating to any advantageous Government, local authority or energy supplier schemes (including energy saving schemes and guidance related to the Green Deal). The installer should ensure that the consumer is shown how to execute key transactions, such as change of supply, selection of tariffs, prepayment, resetting of supply after outage/disconnect and fault reporting.

The Code of Practice could be based on existing codes, such as ERA's "Code of Practice for Face-to-Face Marketing of Energy Supply". BT has considerable experience of best practice in customer installation activities and would be pleased to share this with Ofgem and DECC to ensure that the correct mechanisms are implemented within the suppliers' licences.

To give consumer confidence in the Programme and in the interests of minimising costs, it is essential that the installation of the meter, its communications technology and the IHD are completed successfully on the first (and only) visit, i.e. a high service level should be set on the first time install, with clear accountabilities for executing all installation activities on the visit. The target should be for no re-visits. The installation must include responsibility for meter connectivity to the communications service. We would also recommend that connectivity direct from the meter to the WAN is permitted, rather than via a HAN – this will serve to simplify the service model and responsibilities. We also consider that charging mechanisms should be defined to avoid a consumer backlash.

**Q4** *Have we identified the full range of consumer protection issues related to remote disconnection and switching to prepayment?*

To be addressed in October response.

**Q5** *Do you have any comments on the proposed approach to smaller non-domestic consumers (in particular on exceptions and access to data)?*

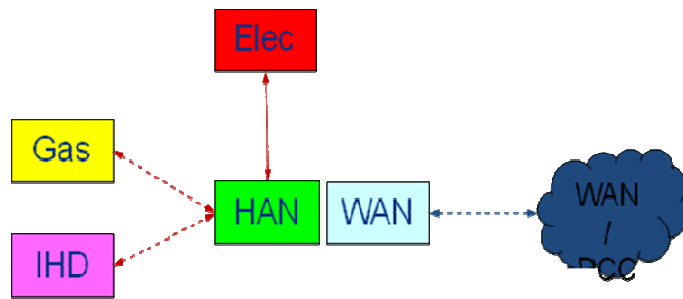
To be addressed in October response.

**Q6** *Do you have any comments on the functional requirements for the smart metering system we have set out in the Functional Requirements Catalogue?*

We are concerned that the Functional Requirements Catalogue describes a smart metering system that will be difficult to deliver in a reliable, cost-effective and secure way on a national scale and does not lend itself to an early rollout of forward-compatible smart metering

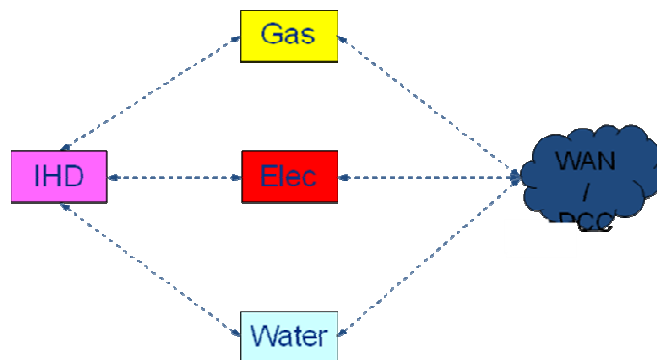
components.

The primary driver for the Prospectus architecture (represented in the figure below) appears to be the requirement to allow the swap out the WAN independently from the HAN. This requirement separates the longevity of the WAN from that of the meter and therefore allows for the WAN module to be upgraded over the life span of the meter. This requirement is not necessary and, moreover, if implemented, would lead to significant incremental cost in terms of installation and maintenance of the meters. Instead, the WAN should be considered integral to the meter and, together, they should form a single asset with a full life span of 15 years.



By integrating secure WAN connectivity directly into the smart meters (as represented in the figure below) it is possible to certify the metrology and the connectivity jointly for the full life of the asset which would in turn lead to a much more straight-forward installation and maintenance programme. The figure also depicts how the WAN would communicate directly with electric/gas/water meters while providing a demarcation bridge point for connection to additional consumer devices and appliances.

Direct WAN connectivity to smart meters, rather than to a HAN Hub, eliminates the ambiguity which would otherwise exist regarding operational responsibility and provides greater assurances regarding Service Level Agreements (SLAs) and Key Performance Indicators (KPIs). Under the Prospectus's proposed architecture, the WAN service provider is responsible merely up to the WAN-HAN interface. This is likely to be physically adjacent to the electricity smart meter but not necessarily near the gas or water smart meter. This puts critical reliance on the communication capabilities of the HAN without any SLA on the WAN provider which is unacceptable as it results in it being unclear who is ultimately responsible for the delivery of smart metering data end-to-end from the meter to the service provider. Further, as well as the HAN Hub being a single point of failure for the entire system, it is required to carry sensitive billing information creating a potential security issue.



Addressing the smart meters directly will also enable supplier led rollout of smart gas meters independently of smart electricity meters if desired. This also means that the gas smart meter WAN connectivity is not affected by any loss of mains electricity supply during operation, as it would be in the proposed architecture. This argument also applies to water meters as existing HAN technologies will not communicate reliably with the majority of water meter locations due

to their distant location at the boundary of the home.

The connectivity of the WAN within the smart metering system needs to be ensured through a series of clearly defined and policed Key Performance Indicators (KPIs). These should include the first time installation success rate, the rate of re-visits to the household during the life of the assets and the connectivity success rate during operation.

KPIs for connectivity need to be defined for delivery of specific metering data and reporting of specific events and alarm messages. For this reason, it is important that the WAN solution be designed first and foremost for retrieving metering information and grid applications securely rather than being a general purpose data carriage network.

The WAN solution selected for the GB smart meter rollout needs to be universal; not only will this make gas and electricity meter infrastructure available across the country, but it should also enable smart water meters, as discussed above, and also empower smart grids. This is achieved by having a technology that can both report advanced smart metering data and events but also has the ability to communicate with monitoring and activation devices within low voltage substations.

In summary, some of the foreseen risks with the system currently described in the Functional Requirements Catalogue are set out in the table below along with suggested mitigations for these expected risks:

<b>Risk</b>	<b>Mitigation</b>
Reliance on a HAN Hub introduces a single point of failure to the customer smart metering system. It also results in a lack of clarity of ownership and how to handle customer care.	Direct WAN connectivity integral to each of the smart meters would remove this single point of failure and ensure stringent Service Levels can be put in place and data can be more tightly secured when kept within the integrated meter.
Failure of the main electricity supply to the HAN Hub would result in failure of communication with the gas and/or water smart meters resulting in denial of service to the customer or home owner.	A direct WAN interface in both the gas and water smart meters would allow their continued connectivity to these utilities even in the event of failure of mains electricity supply
Supplier led rollout is made difficult and therefore expensive for gas or water smart meters as these meters cannot be conducted until after the HAN and WAN modules are installed and provided with an electricity supply.	Direct connectivity between the WAN and all Utility meters by integrating the WAN within every smart meter allows for true supplier led rollout flexibility.
The WAN module may well become obsolete within the lifetime of the meter asset if dependent on a consumer network that is subject to business drivers which take higher priority than smart metering and also due to regular technology updates which re-allocate consumer radio frequencies.	The WAN module integrated into the smart Meter should be certified for the full 15-year life of the asset.

**Q7** *Do you see any issues with the proposed approach to developing technical*

*specifications for the smart metering system?*

We fully support any measures that ensure equipment at consumer premises does not need to change with a change of supplier. Agreeing technical specifications for the consumer premises equipment is an important step to securing this requirement. However there are other interdependencies to consider if this goal is to be achieved.

Under the current proposal, meters rely on the HAN to connect to the WAN. Yet no-one appears to be responsible for the performance of the HAN, therefore what assurance is there that meters will be able to communicate with the DCC, through to users, now and through the lifetime of the meter assets?

Many of the technologies currently being trialled for the HAN as an interim solution are limited in their performance in terms of range, building penetration and susceptibility to interference and degradation over time. We doubt under these circumstances that any entity will be able to provide guarantees over the performance of such HAN technologies. This raises issues over how to complete the technical specifications for customer premises equipment, such as meters, in a way that ensures SLAs can be put in place for the performance of connection of meters to the central network.

We believe an entity, such as the communications service provider, should be responsible for the performance of the connectivity to meters, not just to homes. We therefore believe the specification of meters is not independent of the communications solution and consideration should be given as to how a communications provider can manage their connectivity to the individual meters against agreed SLAs.

We therefore recommend that the specification of customer premises equipment is started in earnest against a broad set of requirements for the end-to-end central communications solution, with the expectation that it cannot be finalised until the communications technology has been selected.

Work to define the user requirements for the end to end smart metering and smart grid system should also start immediately so that the interdependencies with customer premises equipment can be identified, resolved and designed into the customer premises equipment specifications.

Developing customer premises specifications to align with the end to end long term service provision of central communications has other benefits too - it avoids the risk of basing them on the limitations of interim metering technologies and allows full consideration for the requirements of smart grid. Today's smart meters are reliant on meter specifications based on a cellular WAN, which may not deliver the objectives of the long term, including those for smart grid and widespread indoor coverage to meters.

The process we recommend to select the communications services involves:-

- defining the Programme and user requirements/objectives by end 2010, based on end to end SLAs and not designed around any specific technologies;
- defining the OJEU notice such that it encompasses all day one (secure communications) and future (data management) services which may the DCC service providers may be asked to supply;
- issuing an RFI for communications services and seek specification type responses from potential service providers [issue the RFI in Q1, 2011];
- using the procurement process through 2011 to narrow the options and feed into the customer premises equipment specifications;
- Awarding communications service contract, predicated upon the agreed technical specifications for the enduring solution [Q1, 2012].

The approach proposed avoids the issues associated with attempting to agree generic technical specifications from stakeholders representing many different interests and

technologies. It puts the priority on determining the long term end to end solution as the framework for specifying its component parts, including the customer premises equipment.

Through this approach technical specifications on other aspects of the programme, such as meter specifications, can be developed in parallel whilst not causing a critical path dependency.

**Q8** *Do you have any comments on the proposals that energy suppliers should be responsible for purchasing, installing and, where appropriate, maintaining all customer premises equipment?*

To be addressed in October response.

**Q9** *Do you have any comments on the proposal that the scope of activities of the central data and communications function should be limited initially to those functions that are essential for the effective transfer of smart metering data, such as data access and scheduled data retrieval?*

We broadly agree with the proposal, subject to more detailed impact analysis. Essential functions of the DCC should also cover the points below.

The DCC should be responsible for any process changes needed for operation of smart metering communications plus managing any message/data standardisation activities that are required. The DCC should have a governance/community management role – for example in the management of ongoing technical and user groups looking at future enhancements to the DCC (for instance smart grid) and increased scope.

However, before the scope of the DCC is finalised, detailed impact assessments are needed of the pros and cons of central (DCC) versus federated (energy suppliers, DNOs, meter operators etc) data management. The Prospectus recommends that DCC is initially a data carrier. However an entity will need to define how that data is used across all industry parties to ensure that there is consistency in industry processes, e.g. meter registration, and that consumer data is handled consistently and safely. Once defined, the industry bodies will then need to develop systems and systems for generating, collecting, aggregating, processing and storing the data, with an overall checking/gatekeeper role. The question is whether this federated approach is more cost effective, quicker to implement and carries less risk than a centralised approach (managed by the DCC). This impact assessment is needed now, to ensure that either the appropriate supplier licence changes are made or that planning of the centralised role is undertaken for the DCC Licence and Smart Energy Code. If such functions are included within the DCC at a later date (say 2 to 3 years after commencement), then there may be significant transition costs for suppliers and poor investment return. Business continuity and security are needed throughout, which will again add to the cost and complexity of interim solutions.

We agree that the DCC's focus should initially be energy (i.e. not serve other sectors) and that settlement should not be included - the question is the extent to which meter registration, data aggregation/processing/storage are best done in the DCC and when. Experience says not on day one, but after a period of market/service stability - say 5 years for all data services, with meter registration being introduced within 12 to 18 months. There is no point in changing existing and effective operating functions, such as Elexon, ElectraLink and xoserve.

Finally we agree with the design and accreditation roles of the DCC, but suggest that the help desk and security monitoring roles should be undertaken by the service providers with the DCC having capability to review and direct in escalation situations.

We believe that the scope of the DCC and the services it procures should remain dedicated to the needs of the energy sector. If the scope were widened it becomes extremely difficult to predict usage patterns and applications which introduces data privacy, security and performance risk. Furthermore, we believe it is undesirable for such critical national infrastructure to be subjected to alternative commercial imperatives which may jeopardise the delivery of its energy related remit.

Q10	<i>Do you have any comments on the proposal to establish DCC as a procurement and contract management entity that will procure communications and data services competitively?</i>
<p>We support the principle of there being a separate and independent procurement and contract management entity. We believe that this is appropriate given the importance of competition, energy industry focus and licensing, and follows tried and trusted practices.</p> <p>However, the responsibilities of the contract management entity and the service providers need to be clearly defined and adhered to, to ensure that risk is carried by the best equipped parties. For example, the contract management entity should define outcomes (i.e. benefits) and outputs (i.e. SLAs) and not take on responsibility for design, integration or service operation. Equally, the contract management entity should not procure services in such a fragmented way that end to end SLAs and delivery responsibilities are compromised – for example by procuring hosting services separate to communication services. End-to-end integration and service operation of complex critical national programmes must be placed with service providers who have demonstrable experience and expertise in successful delivery. This is certainly true for the initial creation of the DCC's communication services; once these are operational and matured then re-procurement of component parts may be possible, providing that in so doing it does not compromise the initial return on investment for buyers (energy suppliers) and service providers alike.</p> <p>Our view is that communications and data services could, in theory, be procured separately, though we strongly believe that the synergies in infrastructure and management mean that both services could be delivered most cost effectively by a single service provider (most likely as a prime with sub-contractors or as a consortium). Equally, the service providers should respect the assurance, stakeholder management and futures roles of the contract management entity and not endeavour to engage with industry parties to serve their own business purposes.</p> <p>Ofgem is rightly focused on the need for the DCC to enhance the competitive landscape by procuring the best solutions in open competition. The DCC and associated Licences and Codes should rightly be held accountable for ensuring the competitiveness of the Energy industry. However we urge Ofgem not to assume that all elements of competitive communications must necessarily be available from several different parties. We strongly recommend that Ofgem works closely with Ofcom to address (if necessary through Telecommunications regulation) any issues that may arise once the optimum communications solution for smart metering has been specified. After all, in the final analysis competition is sought to ensure enduring value for money of the most suitable solution: it would be counterproductive to select a less suitable suite of solutions (with added complexity and cost) simply because multiple suppliers made it seem more competitive.</p>	
Q11	<i>Do you have any comments on the proposed approach for establishing DCC (through a licence awarded through a competitive licence application process with DCC then subject also to the new Smart Energy Code)?</i>
<p>We agree with this approach. A competitive approach should be used to select the right entity to take the role, offering value for money and expertise. The need for clear auditable terms of reference and openness in its dealings is essential, delivered through the licence and code. We recognise the challenges, however, in selecting a party to fulfil this role who has demonstrable expertise in managing complex national contracts, is experienced in the energy industry and is independent of all suppliers and service providers. It may be that all these characteristics are unavailable, and that the selection of the party for the DCC needs to concentrate first and foremost on industry knowledge and buy in contract or consultancy resources to provide the experience of critical national programme contract management. In addition, the Electronic Communications Code should be taken into account in the establishment of the DCC, particularly with respect to access.</p>	
Q12	<i>Does the proposal that suppliers of smaller non-domestic customers should not be obliged to use DCC services but may elect to use them cause any substantive problems?</i>
<p>To be addressed in October response.</p>	

<b>Q13</b>	<i>Do you agree with the proposal for a Smart Energy Code to govern the operation of smart metering?</i>
<p>Yes. Smart metering is a new service, critical to the country, the industry and most importantly consumers. A dedicated code is needed, embracing smart metering together with other key elements of effective energy management (in particular smart grid) In the interests of timescales, we suggest that the code initially focuses on smart metering and grid applications (to enable early establishment of the DCC) and, if feasible, is extended to smart homes and communities as soon afterwards as practicable.</p>	

<b>Q14</b>	<i>Have we identified all the wider impacts of smart metering on the energy sector?</i>
<p>To be addressed in October response.</p>	

<b>Q15</b>	<i>Is there anything further we need to be doing in terms of our ensuring the security of the smart metering system?</i>
<p>The creation and storage of such extensive data on household energy consumption patterns will generate a plethora of data security challenges. Aside from providing many benefits to the industry, the introduction of a shared communications and data infrastructure offers the potential for threats which will continue to evolve over time.</p> <p>A comprehensive risk assessment, which identifies potential risks and analyses their likelihood and impact, and that represents a 'consensus view', is therefore needed. This can then be used to specify a set of controls that balances the level of assurance provided with the costs of implementing them. A set of security standards must then be published, alongside a governance framework, so that energy suppliers and potential service providers can plan accordingly.</p> <p>The introduction of new functionality to meters such as remote disconnect and the ability to remotely switch between pre-payment and credit, as well as the potential for smart grid functionality, increases the potential impact of security breaches, whilst the accessibility of the communications network increases the likelihood of attempted attacks.</p> <p>The potential risks vary in their level but in many cases can be severe. A collective understanding of these risks needs to be agreed with all of the Programme stakeholders and published. This can then be used to design effective countermeasures.</p> <p>A governance body is needed to continuously review the risk landscape, security strategy and standards to be adopted – this could be the DCC. Alongside this, there is a need for a shared security operations service to manage access control, encryption and key management as well as intrusion detection and response. Managing these functions piecemeal would be expensive and ineffective. Furthermore, there may well be extreme circumstances under which 'crisis' decision-making is needed. Whilst this may well then be 'executed' by the shared security operations service, it will be for the governance body, under the Government's overall direction, to make the necessary decisions (if necessary in ultimate 'arbitration' mode).</p> <p>The staged approach to implementation has the potential to materially increase the overall risk profile if not managed efficiently, and also places a greater onus for mitigating these risks on energy suppliers. These are likely to be ill-equipped to manage this very specialist function and the cost of establishing it, to an acceptable level of assurance, as an interim solution would be high.</p> <p>A centralised security architecture, governed by a set of smart metering and smart grid security principles, must therefore be introduced early enough to protect industry investment of early rollout and rollout post DCC. These principles should focus on "Security by Design", "Defence in Depth" and a "Least Access" policy within the HAN, communication structure(s) and the DCC, aiming to protect the end-to-end infrastructure to acceptable levels. A detailed and holistic risk analysis should be undertaken covering the integration of all the components of the service. This risk analysis should be shared and agreed upon to help the industry specify the controls that will collectively manage known and anticipated threats.</p>	

The creation of the Privacy and Security Advisory Group (PSAG) is a positive step, but must in addition include cross-representation from the industry to ensure timely and relevant input and expertise. To have access to expert knowledge and thus to be effective, it is likely that otherwise vested interests will need to be included within the PSAG.

A governance framework should be implemented as an overarching authority to manage the end-to-end Programme architecture, implementation and enforcement of security standards in line with what is to be expected of an addition to Britain's Critical National Infrastructure.

**Q16** *Do you have any comments on the proposals for requiring suppliers to deliver the rollout of smart meters (including the use of targets and potential future obligations on local coordination)?*

We agree that rollout should be the responsibility of energy suppliers. Mechanisms need to be put in place to coordinate installation activities across potentially multiple suppliers in a geographical area. These should also cover other complexities, such as repeat visits for installation of second meter (gas/electricity/meter) or IHD and a second supplier integrating with the meter installed by the first supplier.

Pre-DCC rollout targets should be intended to define and validate rollout processes and systems, and not to achieve volume targets.

To ensure effective coordination, most importantly in the interests of the consumer experience, an operating model needs to be established across the suppliers (possibly by Ofgem or some other industry body for subsequent novation to the DCC) with supporting information systems (for example a consumer rollout portal). Creation and use of the operating model should be included as an obligation within the modified licences.

**Q17** *Do you have any comments on our implementation strategy? In particular, do you have any comments on the staged approach, with rollout starting before DCC services are available?*

We recognise that there are many good reasons to start meter deployment early, particularly in the knowledge to be gained on the end to end process and systems changes that will be required in a 'Smart' World (e.g. Read to Bill). However we caution that these early deployments will necessarily target the premises which are most straightforward, for example, from a communications perspective. We caution that there are numerous communications technologies that would offer suitable solutions for 60 or even 70% of the target premises. The real challenge is ensuring uniform service is available nationwide at a sensible cost, with the final 30-40% of premises being both technically and commercially challenging. An early 'dash' for the first 70% may well render uneconomic the remainder given these 'left overs' will not be geographically cohesive but be intermingled among the 70% and likely require an alternative national infrastructure to address them. A national infrastructure is wholly affordable when amortised across all the target premises, but becomes less viable as the target premise number declines or if locations are cherry picked. It is for this reason that we caution that while early volume installations may feel supportive of programme acceleration, it runs the real risk of leading to an outcome whereby national deployment is never achieved. Hence we recommend that any meter deployment targets set for energy suppliers are kept relatively low and based on industry process refinement objectives rather than meter installations.

However we would strongly urge that consideration is given either to bringing forward the establishment of the DCC or the procurement of Service Providers (and preferably both) so that:

- a) There is an agreed communications specification, including service interfaces and SLAs, against which suppliers can procure communications service with minimal risk; and
- b) The complexities of novating communications contracts are minimised;
- c) Security can be designed in (as the Prospectus rightly identifies it must be);
- d) The accelerated phased implementation does not have an unintended consequence

of jeopardising ultimate nationwide deployment

We also recommend that more time is allowed for end-to-end testing, business integration proving and implementation of secure business continuity services from the selection of service providers to go live. The Prospectus suggests this could be completed in 6 months. However our experience of implementing critical national infrastructure programmes would indicate a period of at least 12 months to be more prudent, albeit still aggressive – this should be the subject of rigorous implementation planning, now.

In the event that it is impractical to bring forward the establishment of the DCC due to the timescales involved in consultation and creation of the licence and Smart Energy Code, then we recommend that procurement activities to select communications service providers are started in parallel. This approach has been followed successfully with the further deregulation of the electricity industry in the mid-late 90s when the procurement was led by a consultancy with experts appointed from the regional electricity companies. Initially the contract with the service provider was held by the consultancy and then transferred to the contract manager (ElectraLink) once established. No transition difficulties were encountered and the delivery programme was able to commence early and complete successfully, on time.

We also recommend a more rapid approach to the procurement of the communications service provider, achieved by:

- defining programme and user requirements/objectives. Base requirements on end to end SLAs to reflect current and future requirements, ensuring that the limitations of current solutions are not adopted. Consider those SLAs really important to the success of the programme, such as an SLA for the connectivity to meters, rather than homes, an install success rate SLA for connecting and communicating with meters, SLAs for latency, etc.;
- issuing an OJEU notice that encapsulates the full potential scope of the communications service providers (including both secure communications and data management services);
- issuing an RFI for secure communications, and seek specification type responses from potential service providers [issue the RFI in Q1, 2011];
- using the procurement process through 2011 to narrow the options;
- awarding central communications contract with specification based on final solution [Q1, 2012].

Through this approach, technical specifications on other aspects of the Programme, such as meter specifications, can be developed in parallel with the communications service specifications such that the overall implementation timescales are not impacted.

This approach would lead to the following timescales:

Date	Milestone
End 2010	Define user requirements for end to end service
	Define system architecture
	Develop meter and communications specifications
Q1 2011	Issue RFI for central communications service provider
Q3 2011 to Q1 2012	Issue RFP, short list, negotiations Finalise meter specifications
Q2 2012	Award contract for central communications service provider and assign to DCC (DCC anticipated to be in place through an accelerated (alternative) DCC selection process)
Summer 2012	Mandated supplier rollout commences, as proposed by Prospectus, but adopting the enduring solution rather than interim pre-DCC solutions
Q2 2012 to Q2 2013	Enabling rollout from Q2, build, test and commission centralised communications service functions

--

<b>Q18</b>	<i>Do you have any other suggestions on how the rollout could be brought forward? If so, do you have any evidence on how such measures would impact on the time, cost and risk associated with the programme?</i>
------------	---

Establishing both the DCC and the central communications service provider early will create certainty and confidence for ramping up rollout volumes in the timescales identified in the Prospectus. If these timescales are to be retained we propose three parallel work streams:-

- procure DCC through a competitive process;
- develop the regulatory framework;
- procure a central communications provider, starting with an RFI at the end of 2010 based on user requirements not on interim arrangements, requiring respondents to submit specification type responses. Assign contracts to DCC in Q2 2012.

We estimate all three work streams could be completed by Q2 2012, in time for the mandated supplier rollout, which means the enduring solution can be deployed from the outset with full confidence.

The benefits of this approach include:

- avoiding the risk of interim solutions, such as SMS, defaulting to a permanent solution without due consideration to alternative central communications service solutions that can satisfy the longer term objectives of the programme. Such a risk increases with the longer it takes to place the enduring DCC service contracts;
- limiting the cost of establishing local metering-only solutions of limited life and the subsequent cost of migrating local solutions to a central solution;
- increasing certainty for potential communications suppliers, thereby providing encouragement for making early investments against a firm business case.

A new national communications infrastructure could be established to provide coverage to a very high proportion of meter locations by Spring 2013, but coordinated rollout could start from Q2 2012. Growth to a near 100% coverage of meters (not just the exterior of homes!), often located indoors, should be achieved with two to three years of a contract being awarded. There is plenty of evidence to support this speed of rollout. In cellular 3G for example, a rate of 100 base stations per month was achieved. Other site based radio technologies would achieve a similar rate of deployment.

Ofgem eServe should start the procurement of the national communications solution as soon as possible, perhaps by using an independent procurement agent. To save time, an RFI should be published early, based on the overall programme objectives for smart metering and smart grid. This will best inform industry stakeholders of the choices, and pros and cons of each communications solution. Based on selecting the WAN technology for central communications, centralised security and other central services, specifications for the customer premises equipment can be finalised with any interdependences solved in the process.

<b>Q19</b>	<i>The proposed timeline set out for agreement of the technical specifications is very dependent on industry expertise. Do you think that the technical specifications can be agreed more quickly than the plan currently assumes and, if so, how?</i>
------------	--

We welcome the proposal to agree specifications for meters as soon as possible and within the timescales given. Defining technical specifications for the meters alone will do little to narrow the choices for communications solutions, including the HAN and WAN. We recommend consideration is given to the end-to-end system requirements and specifications as part of this process.

Against current plans, we doubt that DCC will be able to appoint communication service providers before 2014. The choice of central communications, including the WAN and SLAs associated with meter coverage and connectivity performance, is closely linked with the specifications of the meters and the choice of home architecture. Therefore we recommend an early definition and selection of the central service provider in order to mitigate risks to

meter rollout timescales.

Given the inter-dependencies, we recommend focused efforts on meeting the challenge in agreeing technical specifications across the end to end service (HAN, WAN, meters, IHDs and central services). This is a critical path activity. Any slippage will delay other programme deliverables.

We believe there are a number of factors that contribute to the risk of timescales slipping:

- there are wide and varying views with respect to technology and specifications for HAN, WAN, meters, IHDs and central communications services, including the configuration of the home architecture;
- the results of meter specification work are helpful and support an interim market, however they do not currently include the specification of the communications technology which is a critical component;
- specification work has not started on the end-to-end solution. This will help to define, on a cost benefit basis, where to place certain functionality and data storage e.g. centrally, at the home, in the meter, etc.;
- the proposed work process will likely result in specifications being influenced in a way that supports the status quo of interim solutions. However it is important not to limit the requirements of the final end-to-end central communications solution by the limitations of current interim solutions;
- we are not clear what the work process is to successfully harmonise the differing views and interests at a detailed specification level;
- time may be wasted creating generic technical specifications for widely differing technology solution approaches rather than narrowing down choices sooner.

Given this environment, we believe there is a risk of delay for agreeing technical specifications.

A more rapid approach could be achieved by:

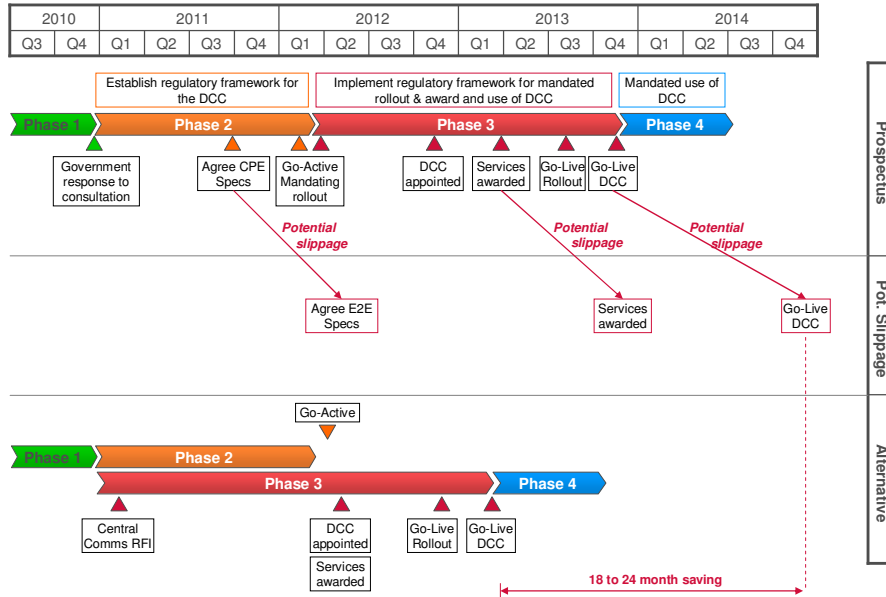
- defining programme and user requirements/objectives. Base requirements on end-to-end SLAs to reflect current and future requirements, ensuring that the limitations of current solutions are not adopted. Consider those SLAs really important to the success of the programme, such as an SLA for the connectivity to meters, rather than homes, an install success rate SLA for connecting and communicating with meters, SLAs for latency, etc.;
- issuing an OJEU notice that encapsulates the full potential scope of the communications service providers (including both secure communications and data management services);
- issuing an RFI for secure communications, and seek specification type responses from potential service providers [issue the RFI in Q1, 2011];
- Using the procurement process through 2011 to narrow the options;
- Awarding central communications contract with specification based on final solution [Q1, 2012].

Through this approach, technical specifications on other aspects of the Programme, such as meter specifications, can be developed in parallel with the communications service specifications such that the overall implementation timescales are not impacted.

This approach would lead to the following timescales:

Date	Milestone
End 2010	Define user requirements for end to end service
	Define system architecture
	Develop meter and communications specifications
Q1 2011	Issue RFI for central communications service provider
Q3 2011 to Q1 2012	Issue RFP, short list, negotiations Finalise meter specifications
Q2 2012	Award contract for central communications service provider and

	assign to DCC (DCC anticipated to be in place through an accelerated (alternative) DCC selection process)
Summer 2012	Mandated supplier rollout commences, as proposed by Prospectus, but adopting the enduring solution rather than interim pre-DCC solutions
Q2 2012 to Q2 2013	Enabling rollout from Q2, build, test and commission centralised communications service functions



Benefits include:

- removes the risk of slippage in agreeing technical specifications
- earlier start for central communications, providing greater certainty sooner, in a way that underpins early investment and rollout;
- avoids mistakes, such as assuming or defaulting to a particular home architecture which then doesn't allow for a service provider to be responsible for the performance of meter connectivity through SLAs;
- limits sunk costs in interim temporary ICT by adopting central communications as soon as possible;
- the final specification is based on the final solution; no wasted effort;
- limits the time and costs invested in short term 'regional' contracts and head end solutions that will need to be replaced by a centralised DCC solution later;
- concentrates the effort around the end to end solution for smart metering and grid, rather than component parts;
- establishes a robust national security assurance solution at the outset;
- places a large part of the effort on potential service providers to develop end to end solution specifications;
- the increase in costs of £200m (identified in the impact assessment as the difference between a Staged Implementation and Full Establishment), which we believe to be underestimated due to the extended period for the interim arrangements associated with late procurement by DCC of the centralised communications.

**Q20** *Do you have any comments on our proposed governance and management principles or on how they can best be delivered in the context of this programme?*

In relation to the governance and management of the smart metering implementation programme, we are broadly in agreement with the suggested governance and management arrangements. We strongly recommend that communications service providers are given the

opportunities to contribute to the Smart Metering Design Group and the Data and Communications Design Group – the importance of smart metering as a critical national infrastructure programme and the need to specify as quickly as possible the communications requirements and specifications mean that industry input should be comprehensive and inclusive. Managing the inevitable different points of view may be challenging, but the benefits of such viewpoints will be considerable. There is also the need to manage consistency between the Design Groups, particularly with regard to the HAN which naturally straddles both. We would also recommend that the Privacy and Security Group takes input from industry security experts, given experiences in other countries of implementing smart metering.

Key aspects of such a critical, national programme are effective stakeholder and communications programmes. To this end we would also suggest that:

- a) All stakeholders are identified and engaged, with a clear plan setting out their respective responsibilities and areas of interest;
- b) The Implementation Co-ordination Group includes industry partners with direct experience of implementing complex, critical, national programmes; and
- c) A Consumer Engagement Group (possibly integrated with the Consumer Advisory Group) is established to address consumer issues (such as privacy) and to implement communications programmes (from now, given the growing commentary emerging in the public domain).

### 3.2. Communications Business Model

Q1	<i>Do you agree that access control to secure centrally-coordinated communications, translation services and scheduled data retrieval are essential as part of the initial scope of DCC?</i>
----	--

Yes. A centralised access control layer should be mandatory to ensure the security of the communications and data infrastructure. This access control needs to be bi-directional to ensure that the industry has specific and role-based access to meter data whilst assuring that scheduled reads, alarms, configuration and firmware updates, as well as real-time messages, are provided only to the correct, validated and authenticated end-points. Access control must adopt the principle of "Defence in Depth" and include basic controls like gateways, firewalls and intruder management, as well as identification, authentication, authorisation and encryption.

It is important to note that access control is not only seen as applicable to the DCC operations, but should be managed by the DCC as an all encompassing framework and should thus cover all internal and external access to any part of the end-to-end system.

Suppliers or potential suppliers will need access to meter data to allow them to provide the most competitive tariff to their current or target consumers. This will require informed consent but must also include accountable access control to ensure that only valid and authenticated bodies have access to the data. Technologically this will prove challenging, with no centralised access control and meter data mastered only within the meters. The Programme should give serious consideration to include services such as registration and change of supplier as centralised functions, presumably as part of a DCC functionality set, from the outset to enable adequate protection.

The inclusion of remote disconnect functionality is a very positive step for the industry, however it also raises serious security concerns. A centralised access control service with enough supporting reference data within the DCC should provide the requisite control and protection necessary to ensure that consumers are protected from wilful or inadvertent threat of or actual disconnection.

Delivering this robust access control within the limited, short term technology and security architecture that is likely to be implemented during the interim period under the staged

approach, will be challenging for energy suppliers, especially when these solutions then need to be subsequently migrated to a central DCC service. This issue needs to be seriously considered, prior to a mandated roll out, to ensure consumer protection.

**Q2** *Do you agree that meter registration should be included within DCC's scope and, if so, when?*

The meter registration process has a tight coupling with communications connectivity and establishing security credentials (via access control mechanisms), hence the processes need to be streamlined and integrated very carefully. If, initially, the DCC does not have responsibility for coordinating the registration process over the Data Transfer Network but this remains with multiple parties (meter operators and suppliers), then end-to-end service integration will be much more complex and will require appropriate testing time before commencement of operation. The interim arrangements that will exist pre-DCC would need to continue, with transition to the DCC as soon as practicable (subject to planning, suggest this would be within the first 12 to 18 months of operation of the DCC). In respect of the legacy data point in the Prospectus, a programme of work should be put in place to resolve this before either interim or DCC arrangements take effect - if not, then there is the risk that this will actually worsen during the interim period before transfer to DCC.

**Q3** *Should data processing, aggregation and storage be included in DCC's scope and, if so, when?*

We agree that the data processing, aggregation and storage should be added to the DCC's scope, but over time once the core communications functions have been established. As outlined in our response to Prospectus Q9, we believe that a more detailed assessment should be undertaken of the costs and risks associated with maintaining these functions across multiple parties as opposed to centrally within the DCC. Subject to this assessment we would recommend that they are brought in to the DCC within 2 to 3 years of commencement of its operations.

**Q4** *Do any measures need to be put in place to facilitate rollout in the period before DCC service availability and the transition to provision of services by DCC, for example requiring DCC to take on communications contracts meeting certain pre-defined criteria?*

Please refer to our response to Prospectus Q17 commenting on the earlier establishment of the DCC. The novation of potentially many contracts across energy suppliers could be challenging for the DCC. Rather the energy suppliers should develop Transition Plans in collaboration with the DCC and should take the responsibility for executing the transition arrangements to the DCC. To simplify transition, it would be helpful if the pre-DCC communications contracts were structured such that there were common service level agreements (and open interfaces) supported by broadly equivalent terms and conditions – a means of achieving these would be to include their definition within the modified supplier licences, following consultation.

We agree with rollout targets for energy suppliers, but recommend that risk/reward elements are built in against key indicators, such as over-delivery and increased consumer satisfaction, and we believe that the key remit of these early roll outs should be to identify and implement process and systems changes required. We recommend that the volume of early installs is managed carefully to ensure that logistic and economic difficulties are not introduced by potentially having a large number of stranded meters before their specifications are baselined.

**Q5** *Do you agree that the licensable activity for DCC should cover procurement and management of contracts for the provision of central services for the communication and management of smart metering data?*

The licence should definitely cover secure communications on a GB-wide basis. It should also be extended to include data services when the associated consultations have been completed and decisions have been made as to the extent to which these are brought into the DCC. We do believe that, initially, the DCC should be focused on communication services, with meter registration following within 12 to 18 months of service commencement. Other data

services should then be added – please refer to our response to Prospectus Q9 for discussion of the pros and cons of a federated versus centralised data management approach.

**Q6** *Do you consider that DCC should be an independent company from energy suppliers and/or other users of its services and, if so, how should this be defined?*

Yes, the DCC should be independent and Not-For-Profit. It needs to manage service providers impartially and for the interests of consumers and energy stakeholders. Its impartiality is enshrined in the Licence. Fundamentally the DCC should be responsible for outcomes within its scope (e.g. service charges) and service levels (e.g. availability of service, data transfer performance).

**Q7** *Do you have any comments on the steps DCC would need to take to be in a position to provide its services and the likely timescales involved?*

In addition to establishing DCC's licence and the Smart Energy Code, the key steps that the DCC would need to take to be in a position to provide its services are:

- implement governance and control arrangements with users of its services;
- define processes for collection and transfer of data to required industry parties;
- prepare output specifications for procurement of communications service providers (please see earlier responses in which we recommend that establishing the DCC and its service providers should be brought forwards);
- oversee the build, test and acceptance of communications solutions (including standards compliance);
- plan service introduction and transition (from pre-DCC services);
- integrate DCC communications services with industry users (including transfer of specific data items to specific service user systems);
- hold model trials with service users (covering functional and non-functional tests) prior to any transition or commissioning activities;
- manage the transition (technical and commercial) to DCC communications services;
- execute communications to all users and stakeholders.

We suggest that the 6 month period suggested in the Prospectus for the above activities is too short for a critical national programme of this size and complexity. We believe that a 12 month timescale is still very challenging but more achievable. As we commented in our response to Prospectus Q17, an alternative approach is to procure the service providers and commence implementation activities in parallel with establishing the DCC. This approach, successfully applied in the electricity deregulation of the 1990s, would enable all the above steps to be initiated earlier than the timescales recommended in the Prospectus and would therefore reduce delivery risks and transitional complexities (compared to having numerous communications contracts that would need to be novated).

**Q8** *Do you have any comments on the proposed approach to cost recovery and incentivisation for DCC?*

For smart metering we suggest that the DCC charges are met by the energy suppliers (in the four categories of activation, standing, volume and general). As the network operators gain benefit from the smart meters (i.e. more accurate and frequent network end point readings) then the energy suppliers should be permitted to discount the charges they pay to the network operators accordingly (based on activation, standing and volume). When smart grid is added the charging regime should change with network operators also being charged directly by the DCC (based on the four categories) to reflect the benefits the network operators will leverage through demand side management and associated SLAs delivered by the DCC. We also recommend that incentives are needed for over-achievement of SLAs and effective management of risks. The DCC should work to a published service rate card with transparency of its operating margin.

### 3.3. Consumer protection

<b>Q1</b>	<i>Do you have any views on our proposed approach for addressing potential tariff confusion? What specific steps can be taken to safeguard the consumer from tariff confusion while maintaining the benefit of tariff choices?</i>
We have no comment to make on this question at this stage.	

<b>Q2</b>	<i>Do you agree with our proposed approach for addressing unwelcome sales activities during visits for meter installation?</i>
We agree with the proposed approach. It is essential that the consumer experience is excellent, from early communications to completed installation, to build confidence in the new services. This is best achieved through a Code of Practice agreed by all suppliers and embedded within their modified licences. The Code will ensure that consumer communications, installation planning, installation visit (including installer identification, handling of difficult access, special provisions for elderly or disabled) and installation feedback are executed consistently and seamlessly, irrespective of supplier.	

<b>Q3</b>	<i>What do you consider as acceptable and unacceptable uses of the installation visit and why?</i>
<p>Installation visits should be only for physical works and consumer familiarisation, not sales - at least for the primary installation visit. If a subsequent visit is needed to fulfil a specific consumer driven order for higher value services (e.g. premium IHD, integration of micro generation products), then limited sales approaches could be included. The installer should be able to supply the consumer with collateral relating to any advantageous Government, local authority or energy supplier schemes (including energy saving schemes and guidance related to the Green Deal). The installer should ensure that the consumer is shown how to execute key transactions, such as change of supply, selection of tariffs, prepayment, resetting of supply after outage/disconnect and fault reporting.</p> <p>The Code of Practice could be based on existing codes, such as ERA's "Code of Practice for Face-to-Face Marketing of Energy Supply". BT has considerable experience of best practice in customer installation activities and would be pleased to share this with Ofgem and DECC to ensure that the correct mechanisms are implemented within the suppliers' licences.</p>	

<b>Q4</b>	<i>Do you agree with our proposed approach to ensuring that the IHD is not used to transmit unwelcome marketing messages?</i>
We agree with the proposed approach. The basic IHD must display energy usage and charging data only (as per specifications to be agreed) and not carry sales content. Any such sales content should be carried via separate channels (email, correspondence etc). If the IHD is used for supplier-specific sales material it makes its use by other suppliers (e.g. gas) or transfer to other suppliers on change of supplier much more difficult. Additional functionality (and marketing / sales content) could be part of an enhanced offering that the consumer would choose to have.	

<b>Q5</b>	<i>Do you agree that consumers should be able to obtain consumption information free of charge at a useful level of detail and format? How could this be achieved in practice?</i>
<p>Consumers are, based on the definition of the Data Protection Act, the Data Subjects and should therefore have appropriate control of what is 'their' data. They should, of course, be able to access their consumption information, free of charge, at a useful level of detail and format. However, we believe that further consideration must be given to the definition of "useful levels", the governance around providing this data and how they will be enabled to undertake this role effectively.</p> <p>Consumers will use this data for many purposes, and will require it in many formats. It must therefore be provided in a manner that is user friendly and easily exportable to a range of devices using a secure, industry standard format.</p> <p>This will be difficult to achieve in practice if consumer data is mastered in the meters themselves, which are not designed for this purpose. A practical answer to this need would be</p>	

for the DCC to hold a secure central repository of this data, which the customer could access when required. This approach would address many of the challenges around data privacy and security, and would assist in supplier switching.

**Q6** *Do you consider that existing protections in the licence are sufficient to ensure that consumers are not remotely switched to prepayment mode inappropriately?*

To be addressed in our October response.

**Q7** *Could provision of an appropriate IHD help overcome meter accessibility issues to facilitate prepayment usage?*

To be addressed in our October response.

**Q8** *What notification should suppliers be required to provide before switching a customer to prepayment mode?*

To be addressed in our October response.

**Q9** *Do you believe that suppliers should be required to provide emergency credit and „friendly credit“ periods to prepayment customers or whether, as now, this can be left to suppliers?*

We have no comment to make on this question at this stage.

**Q10** *Do you consider that an obligation similar to Prepayment Meter Infrastructure Provision (PPMIP) may be required?*

To be addressed in our October response

**Q11** *Is the obligation which Ofgem is proposing to introduce on suppliers to take all reasonable steps to check whether the customer is vulnerable ahead of disconnection sufficient? If not, what else is needed?*

We have no comment to make on this question at this stage.

**Q12** *What notification should suppliers be required to provide before disconnecting a customer?*

To be addressed in our October response.

**Q13** *Do you have any views on the acceptability of new approaches to partial disconnection and how they might be used as an incentive to pay bills?*

To be addressed in our October response.

**Q14** *Do you agree with our approach for addressing issues related to remote disconnection and switching to prepayment?*

To be addressed in our October response.

**Q15** *Have we identified the full range of consumer protection issues associated with the capability to conduct remote disconnection or switching from credit to prepayment terms? If not, please identify any additional such issues.*

To be addressed in our October response.

### 3.4. Data Privacy and Security

**Q1** *Do you have any comments on our overall approach to data privacy?*

*“The customer shall choose in which way consumption data shall be used and by whom, with the exception of data required to fulfil regulatory duties”.*

We believe in principle that this is a positive step and will go some way in alleviating

consumer concerns over data privacy. However, we also believe that there are a number of key points that would need further and careful consideration around data privacy:

- **Privacy by Design:** Data protection must be embedded within the core design of the system, should be introduced early and needs to be in place for the mandated rollout. In practice, therefore, this protection needs to be in place prior to the DCC in order to prevent experiences such as those which occurred in the Netherlands, which gave rise to concerns over privacy that led to its smart metering bill being initially rejected.
- **Consumer Consent:** Whilst we are in agreement that consumer consent for the collection, use and disclosure of meter data should be implemented, we believe that further consideration needs to be given to the requirements of customers who may not be in a position to make informed decisions around what they are consenting to, and the level of consent that they have provided. Enforcement of consumer consent is also a cause for concern as the Data Protection Act, though holistic for personal data protection, may not be granular enough to cover specific meter data privacy. Further, serious consideration needs to be given to how such consent management will be achieved where individuals are not 'digitally enabled' in an environment where meter and meter display functionality will be limited.
- **Data Storage:** Mastering of data within the meters for a period of 12 months in theory provides greater control and ownership to the customers, however it also raises questions around data access and resilience:
  - A number of industry bodies require access to this data, not least the suppliers who would require regular and ad hoc access to data, albeit aggregated in order make key customer and tariff management decisions;
  - Mastering data only within the meters will create a technological as well as process impracticability;
  - Singular data storage with no immediate back-up strategy will create resilience issues where meter data is lost by consumers (either wilfully or inadvertently).

The Programme should therefore give consideration to the possibility of a centralised data store, perhaps within the DCC. We would envisage the DCC working alongside the Information Commissioner's Office (ICO) to create specific meter data protection standards which might be included as part of the DCC license.

- **Data Integrity and Confidentiality:** Storage of large amounts of data locally within the meters also introduces security concerns:
  - The ability to hack into, or interrogate meters, would allow for tampering or misrepresentation of meter data thus causing data integrity issues

There is a further element of concern around sharing of meter data, for example through rental turn-over or change of ownership of property. A change in tenancy status would mean new occupiers having access to meter data from previous incumbents. This could also cause a problem if residences change from domestic to non-domestic status, as this then raises questions over ownership of the data. Clearing down or sanitising this data without any other form of storage or data source would again cause loss of data, especially if the customer wishes their data to move with them.

<b>Q2</b>	<i>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.</i>
-----------	--

We will await guidance from the industry on what levels of data aggregation and frequency of access to smart meter data is required.

However, at this stage, we would like to draw the Programme's attention to the reality that whatever levels and frequency may be agreed, these will have material implications on the security design and cost of operations of the overall solution and especially the 'thickness' of services required to be provided by the DCC. At this stage, it is also important to note that we believe that some DCC functionality will be required throughout the roll-out stages.

**Q3** | *Do you support the proposal to develop a privacy charter?*

Yes, a privacy charter should be developed to reduce public concerns, meet the expanding amount of digital information and thereby provide a framework for governance of smart metering operations. However, in recent times, the privacy debate has moved away from surveillance and analogue interception, into networks capable of carrying millions of packets of personal data around the world to various companies and other third parties.

A privacy charter is therefore needed that takes account of these changes. To enable such a charter, the industry needs to be prepared to report against conformance with the charter, which will therefore need defined processes to underpin it and to deliver that adherence. To ensure such accountability, a method for auditing is also required. In the longer term, we believe that the DCC is best placed to oversee and manage compliance against the privacy charter, however in the interim, this will be problematic and a suitable body will need to be appointed to undertake the enforcing role.

**Q4** | *What issues should be covered in a privacy charter?*

The following issues need to be considered in any privacy charter:

- how to ensure anyone handling or processing data is held accountable and accepts ownership of risk;
- how to guarantee individuals are providing informed consent in a multi-stakeholder environment;
- how to ensure information is accurate, available and has the ability to be corrected;
- how to assert all processes and the existence of services requiring access to consumer data are transparent;
- how to promise consumer safety and privacy, but be sure to limit the collection of the data to the minimum amount of personal information for the task required;
- to what extent does the system manage consumer demand for data in the preference they wish;
- how to enforce permissions for access to data that ensures the requirement of consent for data use or disclosure;
- how to reassure the public that any data held cannot disadvantage anyone, but enable the consumer to challenge the system as to what data is held and for what purpose;
- how to guarantee expectations to the charter (such as data required for national security purposes or competition) that does not infringe on the principles of the charter.

In addition, we would expect that any obligations on the consumers would be included in the terms and conditions in the agreements between the consumers and suppliers or third parties.

**Q5** | *Do you agree with our approach for ensuring the end-to-end smart metering system is appropriately secure?*

The Prospectus does not make it clear how the smart metering system will guarantee that the end-to-end solution will be secured, especially in terms of the 'multiple staged' overall deployment.

We offer the following comments:

<ul style="list-style-type: none"> <li>• There is a need for a central security governance authority responsible for the protection of the smart metering system that will ensure that security standards are agreed, adhered to, and independently audited. This body will facilitate co-operation across the industry, and will ensure that public and industry perception of the effectiveness of these standards remains positive.</li> <li>• All stakeholders agree that interoperability is a key driver to the success of an end-to-end secure system. The smart metering system requires a central monitoring and brokering service to ensure all smart metering elements are able to interoperate in a secure manner from the outset within a rationalised process framework with its associated cost savings for all parties.</li> <li>• The approach of the Security Policy Framework (SPF) followed so far, that includes a CESG IAS 1 technical risk assessment with its inbuilt leaning to the confidentially perspective of technical security, does not appear to provide a truly holistic security strategy and is unlikely to be understood or complied with by either the supplier and consumer communities. Any approach for securing a system end-to-end must include the availability and integrity impact perspectives as well as people and process controls perspectives, if a holistic, and end to end, security solution is to be achieved.</li> <li>• Although privacy is the major focus and concern for the Programme, equal consideration must be given to integrity and availability of the service from a supplier and consumer perspective. Integrity and availability, as well as privacy, should therefore also be major drivers in securing any system.</li> </ul> <p>We recommend that the HMG Security authorities need to be more fully engaged than at present, along with all industry parties and all as members of the PSAG, to reach an agreement that the end-to-end system will be appropriately secure.</p>
---

### 3.5. Implementation Strategy

<p><b>Q1</b> <i>Do you have any comments on our proposed governance and management principles or on how they can best be delivered in the context of this programme?</i></p>	<p>In relation to the governance and management of the smart metering implementation programme, we are broadly in agreement with the suggested governance and management arrangements. We strongly recommend that communications service providers are given the opportunity to contribute to the Smart Metering Design Group and the Data and Communications Design Group – the importance of smart metering as a critical national infrastructure programme and the need to specify as quickly as possible the communications requirements and specifications mean that industry input should be comprehensive and inclusive. Managing the inevitable different points of view may be challenging, but the benefits of such viewpoints will be considerable. There is also the need to manage consistency between the Design Groups, particularly with regard to the HAN which naturally straddles both. We would also recommend that the Privacy and Security Group takes input from industry security experts, given experiences in other countries of implementing smart metering.</p> <p>Key aspects of such a critical, national programme are effective stakeholder and communications programmes. To this end we would also suggest that:</p> <ol style="list-style-type: none"> <li>a) All stakeholders are identified and engaged with, with a clear plan setting out their respective responsibilities and areas of interest;</li> <li>b) The Implementation Co-ordination Group includes industry partners with direct experience of implementing complex, critical, national programmes; and</li> <li>c) A Consumer Engagement Group (possibly integrated with the Consumer Advisory</li> </ol>
--	---

Group) is established to address consumer issues (such as privacy) and to implement communications programmes (from now, given the growing commentary emerging in the public domain).

**Q2** *Are there other cross-cutting activities that the programme should undertake and, if so, why?*

We suggest that a number of additional cross-cutting activities are considered.

The first of these is technology and service innovation. Certainty of delivery is of paramount importance and that naturally leads to the deployment of existing and proven technologies and service models. We fully support this. However, areas for innovation will emerge and these may sit across many different suppliers and providers. To maximise the benefits realisable through innovation, a cross-industry view needs to be taken, facilitated by Ofgem/DECC. We therefore recommend an Innovations Board, chaired by Ofgem/DECC with participants from the Design Groups and industry experts.

In the delivery of the programme there are opportunities for the sharing of resources (information as well as people) to help overall coordination and to manage costs. These may cover a joint national programme requirements and design authority, the adoption of common programme management methods (for instance use of MSP and Prince2) and tools and shared test and integration centres. Such mechanisms have been used successfully in the past with complex national programmes.

**Q3** *Do you agree with our proposal for a staged approach to implementation, with the mandated rollout of smart meters starting before the mandated use of DCC for the domestic sector?*

We recognise that there are many good reasons to start meter deployment early, particularly in the learning to be gained on the end to end process and systems changes that will be required in a 'Smart' World (e.g. Read to Bill). However we caution that these early deployments will necessarily target the premises which are most straightforward, for example, from a communications perspective. We caution that there are numerous communications technologies that would offer suitable solutions for 60 or even 70% of the target premises. The real challenge is ensuring uniform service is available nationwide at a sensible cost, when the final 30-40% of premises are both technically and commercially challenging. An early 'dash' for the first 70% may well render uneconomic the remainder given these 'left overs' will not be geographically cohesive but will be intermingled among the 70% and likely require an alternative national infrastructure to address them. A national infrastructure is wholly affordable when amortised across all the target premises, but becomes less viable as the target premise number declines. It is for this reason that we caution that while volume early installations may feel supportive of programme acceleration, it runs the real risk of leading to an outcome whereby national deployment is never achieved.

Hence we recommend that any meter deployment targets set for energy suppliers are kept relatively low and based on industry process refinement objectives rather than meter installations.

However we would strongly urge that consideration is given either to bringing forwards the establishment of the DCC or the procurement of Service Providers (and preferably both) so that:

- a) there is an agreed communications specification, including service interfaces and SLAs, against which suppliers can procure communications service with minimal risk; and
- b) the complexities of novating communications contracts are minimised;
- c) security can be designed in (as the Prospectus rightly identifies it must be);
- d) the accelerated phased implementation does not have an unintended consequence of jeopardising ultimate nationwide deployment.

We also recommend that more time is allowed for end-to-end testing, business integration proving and implementation of secure business continuity services from the selection of

service providers to go live. The Prospectus suggests this could be completed in 6 months. However our experience of implementing critical national infrastructure programmes would indicate a period of 12 months to be more prudent – this should be the subject of rigorous implementation planning, now.

In the event that it is impractical to bring forwards the establishment of the DCC due to the timescales involved in consultation and the creation of the licence and Smart Energy Code, we would recommend that procurement activities to select communications service providers are started in parallel. This approach has been successfully taken in the past with the deregulation of the electricity industry in the mid 1990s when the procurement was led by a consultancy with experts appointed from the regional electricity companies. Initially the contract with the service provider was held by the consultancy and then transferred to the contract manager (ElectraLink) once established. No transition difficulties were encountered and the delivery programme was able to commence early and to complete successfully, on time.

**Q4** *Do you have any comments on the risks we have identified for staged implementation and our proposals on how these could best be managed?*

In the table below, we identify the primary risks with the proposed staged implementation approach and suggest mitigating actions:

<i>Risk</i>	<i>Mitigation</i>
Delay in DCC having effective management control due to complexity in novating pre-DCC communications contracts.	Earlier establishment of DCC. Agreement of communications requirements and solutions before rollout of smart meters. Earlier placement of service provider contracts in parallel with establishing the DCC.
Lack of consistent GB-wide SLAs due to deployment of mixed communications technologies and services.	Mandate GB-wide SLAs and implement single solution set.
Exposure to cyber security threats due to mixed technologies being deployed (both at service start and upon competitive re-procurement) or novated (from pre-DCC).	Minimise mix of communications solutions and providers through reducing number of pre-DCC communications contracts and utilising a national re-procurement strategy (while retaining competitive dynamic).
Delay in rollout of smart meters due to uncertainties around full communications requirements and standards and associated commercial risks in transferring to DCC.	Earlier establishment of DCC. Agreement of communications requirements and solutions before rollout of smart meters.
Delay in end-to-end service testing and business integration leading to timescale overruns or premature service commencement.	Allow more time between selection of service providers and testing, acceptance and commissioning of services.
The staged approach may create a legacy installed base of meter interim communications solutions that will bias DCC's procurement of the enduring solution in favour of the interim providers.	Bring forwards the procurement of the enduring solution, and focus the pre-DCC roll out on proving process and solutions and not on achieving a volume target.

**Q5** *Do you have any other suggestions as to how the rollout could be brought forward, including the work to define technical specifications, which relies on industry input?*

We fully support the work on developing technical specifications for the meters and recommend the programme works in parallel on other aspects of the end to end solution, such as the IHD, HAN, WAN and central services. Finalising specifications for the meters will be extremely helpful but there are interdependences between various solution elements that we believe need to be considered in parallel.

- Until the WAN is selected, it is impossible to complete the technical specifications for the meters, the communications hub, the IHD or the central services. The

communications provider must be responsible, through SLAs, for the performance of the connectivity to the meters. For instance, should connectivity to the meters be via the HAN or direct to the WAN?;

- The end to end risks to be managed by the central communications provider need to be defined;
- Responsibility for the performance of the HAN needs to be defined;
- Only when there is an understanding and agreement of an end-to-end solution architecture should decisions be made as to where data and functionality should reside, i.e. within the central communications services, within the communications hub or within the meter. Such decisions should also take into account the associated costs.

Specification of other elements of the end to end solution therefore needs to be developed to keep pace with and influence the final meter specifications.

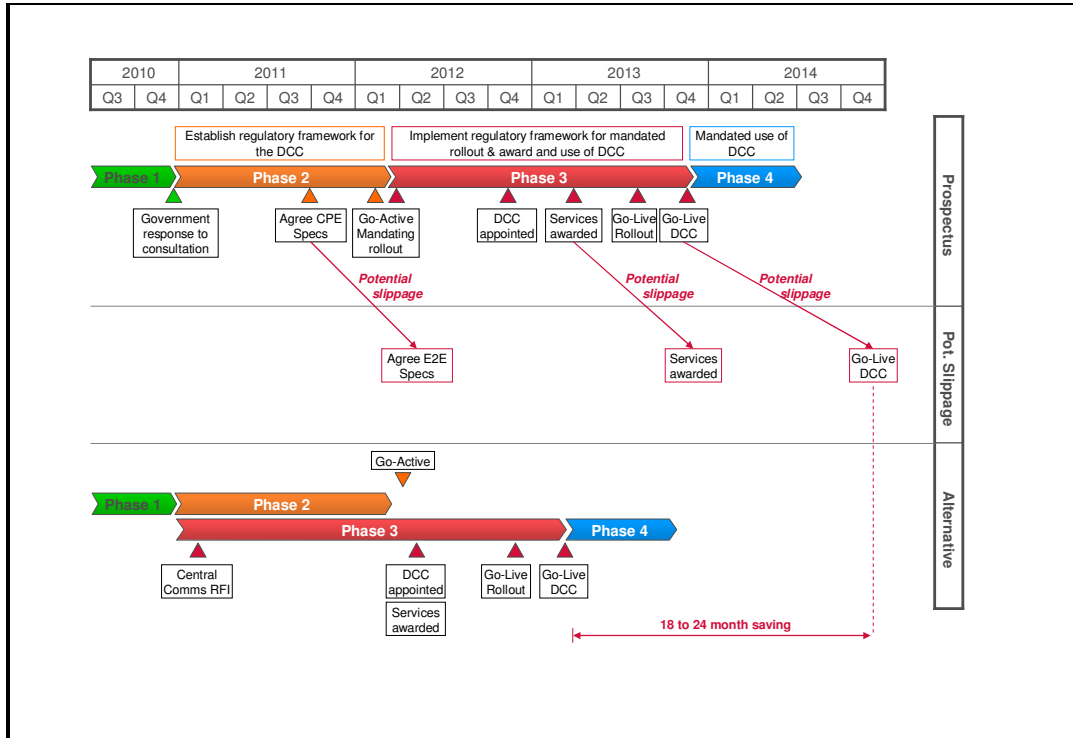
We recommend a re-ordering of the Programme's activities to address these issues.

- Defining programme and user requirements/objectives. Base requirements on end to end SLAs to reflect current and future requirements, ensuring that the limitations of current solutions are not adopted. Consider those SLAs really important to the success of the programme, such as an SLA for the connectivity to meters, rather than homes, an install success rate SLA for connecting and communicating with meters, SLAs for latency, etc.;
- Issuing an OJEU notice that encapsulates the full potential scope of the communications service providers (including both secure communications and data management services);
- Issuing an RFI for secure communications, and seek specification type responses from potential service providers [issue the RFI in Q1, 2011];
- Using the procurement process through 2011 to narrow the options;
- Awarding central communications contract with specification based on final solution [Q1, 2012].

Through this approach, technical specifications on other aspects of the Programme, such as meter specifications, can be developed in parallel with the communications service specifications such that the overall implementation timescales are not impacted.

This approach would lead to the following timescales:

Date	Milestone
End 2010	Define user requirements for end to end service
	Define system architecture
	Develop meter and communications specifications
Q1 2011	Issue RFI for central communications service provider
Q3 2011 to Q1 2012	Issue RFP, short list, negotiations Finalise meter specifications
Q2 2012	Award contract for central communications service provider and assign to DCC (DCC anticipated to be in place through an accelerated (alternative) DCC selection process)
Summer 2012	Mandated supplier rollout commences, as proposed by Prospectus, but adopting the enduring solution rather than interim pre-DCC solutions
Q2 2012 to Q2 2013	Enabling rollout from Q2, build, test and commission centralised communications service functions



The benefits of a parallel approach to establishing regulation, the DCC and the central communications service providers are:

- saving of more than 18 months from the estimated delayed DCC go live, from end 2014 (slippage from the proposed Autumn 2013 due to timescales needed to procure service providers) to Q2 2013. Cost savings attributed to this shortened timescale are applicable;
- reduced risk of various interim WAN, HAN and head-end solutions becoming permanent, with enduring communications solutions being postponed for up to five years and up to two years after the establishment of the DCC code/contract administrator. This is contrary to DECC's earlier decision, through consultation, for Central Communications;
- cost and time avoidance associated with removing the need for investment in and establishing local metering only (no smart grid) solutions of limited life. A significant part of interim solution investment could become obsolete once the enduring communications goes live;
- greater technical certainty is delivered sooner, encouraging investment and ramp up in rollout volumes;
- Longer duration of certainty enabling potential communications suppliers a better investment case early on, likely resulting in a lower long term Total Cost of Ownership. Any new infrastructure for smart metering can be deployed earlier to meet 'every meter' target.

RFI responses, including recommendations on technology and SLAs, will enable the tightening up of requirements and further development of technical specifications.

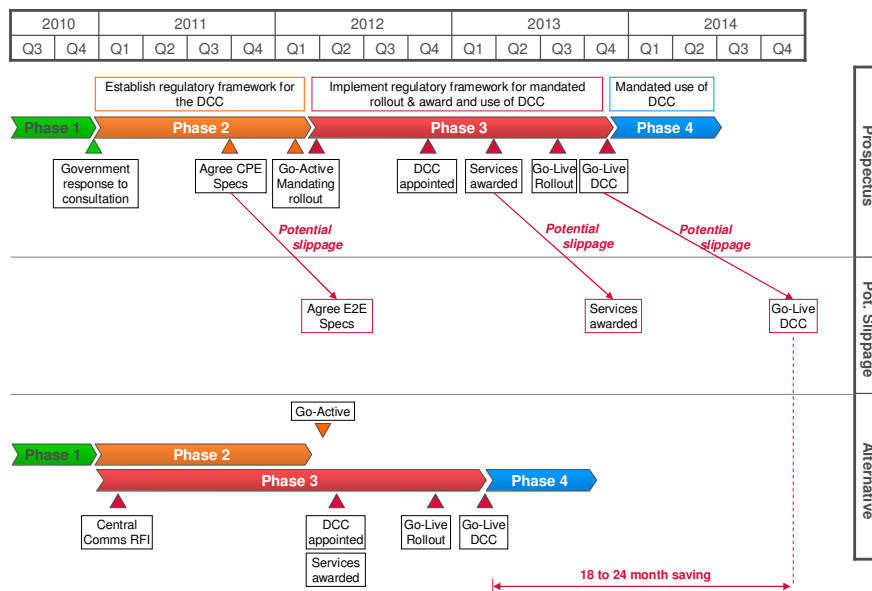
This approach does not detract from the proposed work on agreeing meter specifications. Indeed, it removes the activity from the critical path and ensures meters, once specified, will be compatible with the long term central communications solution delivered through the DCC.

**Q6** *Do you agree with our planning assumption that a period of six months will be needed between the date when supply licence obligations mandating rollout are implemented and the date when they take effect?*

We have no comment to make on this question at this stage.

Q7	<i>Do you have any comments on the activities, assumptions, timings and dependencies presented in the high-level implementation plan?</i>
<p>We agree that the high-level implementation plan is a structured way of implementing the Programme with minimum regulatory and legal risk. However, the serial nature of the activities means that the programme will follow a protracted critical path where slippage of any activity has a knock on impact to the next activity.</p> <p>We believe there are two main areas where slippage is a real risk:</p> <ol style="list-style-type: none"> <li>a) developing the functional requirements and technical specifications;</li> <li>b) appointing the DCC and DCC service providers.</li> </ol> <p>As a result of slippage in either or both of these two areas, central communications might not be in place until the end of 2014.</p> <p>Further, we are concerned that the Prospectus recommends early roll-out using a fully competitive approach when this will most likely result in multiple WAN and HAN solutions thus creating a complex environment for the DCC to inherit when it is finally appointed.</p> <p><b>Reasons for potential delay in the high-level implementation plan:</b></p> <p>It is important that the functional requirements and technical specifications include the end-to-end services provided by the central communications provider, including the WAN and central security arrangements. Given this scope, it is unlikely to be completed by Summer 2011. A more realistic date for this wider remit would be early 2012. Delays will promote an accelerated rollout of a mix of interim WAN and HAN solutions, storing up problems for DCC to resolve within the enduring solution.</p> <p>We also doubt that the DCC could procure and award contracts to service providers within 6 months of the DCC licence being granted. Insufficient time has been allocated for the new services, once contracted, to be developed and tested prior to going live. The DCC must be able to engage with industry, write and implement a procurement process; integrate various interim solutions, novate contracts and manage the risk and complexity associated with launching and integrating a long term centralised solution. We believe 12 to 18 months as a minimum will be required. Evidence for this recommendation can be drawn from many public procurement exercises.</p> <p>Taken together, we estimate Go-Live DCC could be delayed until the end of 2014. Under this scenario, various interim smart metering solutions are likely to become de facto permanent, contradicting the decision by DECC to implement Central Communications.</p> <ul style="list-style-type: none"> <li>• Defining programme and user requirements/objectives. Base requirements on end to end SLAs to reflect current and future requirements, ensuring that the limitations of current solutions are not adopted. Consider those SLAs really important to the success of the programme, such as an SLA for the connectivity to <u>meters, rather than homes</u>, an install success rate SLA for connecting and communicating with meters, SLAs for latency, etc.;</li> <li>• Issuing an OJEU notice that encapsulates the full potential scope of the communications service providers (including both secure communications and data management services);</li> <li>• Issuing an RFI for secure communications, and seek specification type responses from potential service providers [issue the RFI in Q1, 2011];</li> <li>• Using the procurement process through 2011 to narrow the options;</li> <li>• Awarding central communications contract with specification based on final solution [Q1, 2012].</li> </ul> <p>Through this approach, technical specifications on other aspects of the Programme, such as meter specifications, can be developed in parallel with the communications service specifications such that the overall implementation timescales are not impacted.</p> <p>This approach would lead to the following timescales:</p>	

Date	Milestone
End 2010	Define user requirements for end to end service
	Define system architecture
	Develop meter and communications specifications
Q1 2011	Issue RFI for central communications service provider
Q3 2011 to Q1 2012	Issue RFP, short list, negotiations
	Finalise meter specifications
Q2 2012	Award contract for central communications service provider and assign to DCC (DCC anticipated to be in place through an accelerated (alternative) DCC selection process)
Summer 2012	Mandated supplier rollout commences, as proposed by Prospectus, but adopting the enduring solution rather than interim pre-DCC solutions
Q2 2012 to Q2 2013	Enabling rollout from Q2, build, test and commission centralised communications service functions



Whilst this needs to be managed carefully, we estimate a saving of up to 18 months compared to the Prospectus high-level implementation plan together with the risks we see with that plan. The table below explains:

Date	Prospectus Milestone	Alternative approach
Spring 2011	Enhanced consumer protections introduced as required	Issue RFI for end to end solution, including central data, communications and security). This will help to define/narrow technical specifications for a workable national solution.
Summer 2011*	Functional requirements and technical specifications confirmed subject to outcome of any notification under the EU Technical Standards and Regulations Directive	Issue RFP for communications services in line with EU procurement standards
Early 2012	Go-Active: Supply licence modifications mandating rollout implemented	End to End functional requirements and technical specifications confirmed

		subject to outcome of any notification under the EU Technical Standards and Regulations Directive
Spring 2012	Regulatory framework relating to DCC implemented	<ul style="list-style-type: none"> <li>i) Regulatory framework relating to DCC implemented</li> <li>ii) DCC appointed, DCC licence granted</li> <li>iii) Award Central Communications service provider, and assign to DCC</li> </ul>
	Competitive licence application process for DCC licence	
Summer 2012	Go-Live Rollout: Mandated supplier rollout commences	Go-Live Rollout: Mandated supplier rollout commences
Autumn 2012	DCC licence granted	
Spring 2013	DCC service providers appointed	DCC trialling and testing complete
Autumn 2013	DCC trialling and testing complete	
	Go-Live DCC: Mandated use of DCC for domestic customers	

A minimum saving of £200m is possible through an accelerated approach to full establishment - see IA (1.94bn under full establishment versus 2.14bn under staged implementation), bearing in mind £200m assumes no slippage to the procurement of central communications by DCC and could therefore be under-estimated.

Our recommendations are based upon the following analysis:

The Prospectus promotes an accelerated rollout of a mix of interim WAN and HAN solutions.

This appears to be at odds with the findings in the December 2009 DECC consultation. The consultation recommended a central communication provider market model (CCP).

The rationale for this recommendation was based on the comparison of costs between three models; fully competitive, central communication provider and regional roll out.

Regional roll out was rejected, although delivering the highest net benefits, on grounds it would be open to legal challenge and delay the process, or indeed never get started.

DECC reached a conclusion that a fully competitive solution would add cost and complexity to the programme, specifically stating that a competitive solution would create duplication in systems.

The impact assessments show an increase in set up charges of £760m between central communications and a fully competitive model.

It is surprising therefore that only 9 months later the Prospectus is proposing to introduce a fully competitive model in the interim ahead of establishing a central communications provider market model. This proposal would clearly introduce the duplication identified previously by DECC and seek to pass this complex system of communications and data systems to a new market entry to manage, with contracts it had not negotiated.

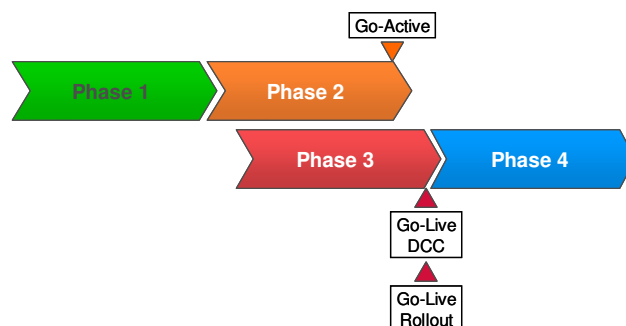
This would appear to ignore the previous assessments conclusion and introduce unnecessary

costs.

**Q8** *Do you have any comments on the outputs identified for each of the phases of the programme?*

We generally agree with the outputs defined for each of the phases. The serial nature of the activities does mean that the adoption of central communications is on the critical path and subject to the impact of any slippage. Furthermore, we believe the time for DCC to procure the services is too optimistic. Under the original proposal, we doubt central communications could be in place before the end of 2014.

We would recommend consideration is given to parallel phase 2 and phase 3 activities as depicted in the diagram below. This would mean regulation, the DCC and central communications is in place together around Spring 2012, reducing the overall timescales of a centralised solution by approximately 2 years.



**Phase 2 outputs**

We agree with the outputs defined in the Prospectus. The functional requirements and specifications for the smart metering system should include not just customer premises equipment, but be scoped further and include the end to end central communications service. This will ensure any rollout is fully interoperable end to end.

**Phase 3 outputs**

By parallel tracking, we suggest it may be possible to coincide the milestones Go-Live DCC with the Go-Live Rollout. This means that the regulatory framework becomes effective alongside the service providers being appointed. Once the DCC is established, the service provider contracts are assigned to the DCC. This means that the Go-Live Rollout is based on the final solution for central communications, under the full governance of an active DCC.

### 3.6. In-home Display

**Q1** *We welcome views on the level of accuracy which can be achieved and which customers would expect, in particular in relation to consumption in pounds and pence.*

The detail or precision of the display must be meaningful to the consumer to provide them with sufficient feedback to show the results of changing behaviour. This can be provided in two ways. First by providing a spot usage rate to show the effect of turning specific devices on or off. It is likely that this data does not have to be highly accurate as the comparator is important rather than the absolute value.

The second type of display is a cumulative display of usage to show trends over time. Again, a high level of accuracy might not be required in this instance. However, there is a risk that the consumer might compare the IHD information with their billing information. If there is a significant inaccuracy in the IHD display then this could generate a significant number of

additional calls to retailers from consumers querying their bill. Therefore, the level of accuracy needs to be set so that over a reasonable period, say a year, that the IHD is not likely to be at variance with any remote system produced bill. We would also suggest that at install time the consumer is made aware that the IHD is primarily intended to show trends in usage and not as a means of validating the bill.

Given that the maximum hourly charge for power is likely to be less than £5 (based on a price of 12p per kWh for electricity and a maximum demand of 25 kWh), precision to the nearest pence (or 5 pence) would seem adequate for the hourly or instantaneous results (giving an accuracy of better than 95%). There would appear to be no benefit of sub pence display to the majority of consumers.

**Q2** *We welcome evidence on whether information on carbon dioxide emissions is a useful indicator in encouraging behaviour change, and if so, how it might be best represented to consumers.*

The means of calculating and displaying emissions information is an issue that needs careful consideration. Consumers will have different perceptions of what is high or low usage. This has been shown in the car excise duty arena where the g/km CO<sub>2</sub> metric is not widely understood. It is therefore important that the levels of emissions are expressed in every day terms meaningful to consumers. One possibility is to have pre-set profiles for household types against which comparisons can be made in real time, with consumers able to adjust their profiles. Another is for the profiles to present equivalence examples, such as consumption for use of heating over consumer selected period being equivalent to CO<sub>2</sub> absorption of x number of trees. Any local micro-generation would not present as a CO<sub>2</sub> credit as it is not possible to relate to the way in which that energy is used (and therefore CO<sub>2</sub> generated).

**Q3** *We welcome views on the issues with establishing the settings for ambient feedback.*

From trial experience, where a display shows different colours depending on energy usage, consumers were much more aware of when high power usage was happening and would take steps to understand why. The settings were made by the user but could be system optimised.

However, there are a number of issues with providing such a display. These include:

- Will the display be based on relative usage (showing decreases) or absolute values (showing consumption relative to a benchmark)?
  - If consumers have high electricity usage, even significant changes in their behaviour may not result in discernable changes;
  - Consumers with low usage (e.g. in a well insulated home) may become complacent even though there are changes they could make to lower their consumption further;
  - Ambient displays would not encourage consumers to continuously improve their energy usage as once consumers achieve a green light, behavioural change will tend to plateau.
- What will the ambient displays be profiled against? Property type, location, age? We would expect that a range of profiles would need to be available to the consumer;
- Will two ambient displays be required for each energy type (gas and electric) or will a combined display be used?;
- What level of additional processing power and software complexity will be needed to calculate the ambient settings for display? Will these have a significant cost impact upon the IHD?;
- Consideration needs to be given to the possibility of ambient lighting causing unwelcome behaviours. For example, vulnerable elderly people may be discouraged from turning on the heating during periods of cold weather if doing so results in a negative ambient display;
- Will the use of different colours for the various day of use tariffs be helpful to consumers?

**Q4** *Do you think that there is a case for a supply licence obligation around the need for appropriately designed IHDs to be provided to customers with special requirements,*

	<i>and/or for best practice to be identified and shared once suppliers start to roll out IHDs?</i>
<p>We support the principle that consideration needs to be taken of people with special needs. One way of doing this would be to have a smaller number of specialist in-home displays that consumers could choose that could deal with their needs.</p> <p>Specialist organisations such as Age Concern, RNIB etc should be consulted on how these layouts could be made more meaningful and readable by those who would not be comfortable or able to engage with the standard offering. The results of these consultations should be embodied into a set of best practice guidelines which suppliers should be expected to adhere to.</p> <p>The assumption that these solutions are going to be more expensive need not necessarily be true. Simple solution are often the best, this can be compared with the large display and button phones that are available. This supports the view that IHDs should be available from other sources that just the retail energy companies and that ubiquitous supply of one device may not be the right answer.</p>	

<b>Q5</b>	<i>We welcome evidence on whether portability of IHDs has a significant impact on consumer behavioural change.</i>
<p>The ability to move the display around the premises would be beneficial, as this would allow for the quick wins (around the home) which are probably the most substantial wins in the long terms and bring about a change in consumer behaviour. If this can be maintained then the benefits will be long term and the advantage of the display for this type of benefit is likely to reduce slightly anyway.</p> <p>The advantage of a portable display is that the consumer in the long term is likely to find a favoured location that is most convenient which may or may not have a power socket accessible. This will continue to provide them with a view of their consumption and provide the long term information they need to manage their usage such as potential tariff benefits etc.</p> <p>An option worth investigation is whether the provision of a small solar panel within the device similar to those in calculators would be sufficient to recharge a local store to power the device. Alternatively, the ability for aftermarket IHDs to be purchased by consumers may allow them to buy portable IHDs if they require one (or more). The consumer will need to be advised that if moving the IHD they need to ensure that it retains connectivity to the meter (similar to moving a portable laptop utilising wireless connectivity).</p> <p>We will investigate whether evidence can be made available to support these recommendations.</p>	

<b>Q6</b>	<i>Do you agree with the proposed minimum functional requirements for the IHD?</i>
<p>The IHD has two purposes:</p> <ul style="list-style-type: none"> <li>• To enable consumers to interact with some basic functionality of the meter (e.g. pre-payment top-up and gas or electricity reconnection acknowledgement);</li> <li>• To provide a display of information about a consumer's energy (and in the future water) usage.</li> </ul> <p>The first of these will be required where consumers will not be able to easily access the meter itself, and as such should be included in the minimum functionality.</p> <p>The second is to support consumers in changing their energy usage behaviour by providing feedback to them. To this end, there is a greater range of functionality that can be considered. However, this additional functionality will increase the cost of devices and therefore presents a trade-off between the costs of providing devices by the suppliers against the level of engagement of consumers to deliver the behavioural change necessary.</p> <p>Although the research evidence into the use of IHDs by consumers is mixed, there is some evidence that most consumers use the display for the first few months allowing them to reduce their energy usage and make savings. However, in the long run, many consumers stop using their devices and simply consign them to the cupboard drawer. In light of this rapid tail-off of usage of the IHD, we recommend that the IHD provided as part of the smart metering rollout should provide a very basic level of information display. The basic IHDs should have the following characteristics:</p> <ul style="list-style-type: none"> <li>• The display needs to be portable if possible to allow for ease of locating in the home,</li> </ul>	

so long battery life is important;

- The display needs to be easy to read and easily configurable to the consumers needs and wishes, e.g. no point in showing gas consumption if the consumer does not have gas;
- The units that the consumer sees need to be easily changed to meet their needs, some will understand Kwh but other may wish pence per minute/hour/day etc.;
- Careful consideration needs to be given to how much information is displayed and how it is displayed to ensure its intelligibility. It is recommended that the Programme issue guidelines on this to ensure a minimum standard is provided on the “free” IHDs.

However, smart meters should also provide open, secure interfaces to their data to allow a market in after-market IHDs and other devices (e.g. TV Set-Top boxes) that would allow consumers who are dissatisfied with the base level of information provided but remain motivated to make behavioural change and so wish to “upgrade” their IHD. These external devices may also be able to use additional information from the Internet via a broadband connection to enhance the display. The types of additional functionality that the aftermarket devices might provide includes:

- selection of a usage profile such that consumers can compare their profile day to day;
- highlighting periods of cheaper electricity tariff. A traffic light system off-tariff may be effective. Different time of use tariffs may be shown in different colours to enable ease of notification to consumers;
- the presentation of carbon emissions could also be provided for more ecologically conscious consumers. However, it is acknowledged that the calculation of this information is far from straightforward.

The free IHD, which might have a short life, needs to be of low cost to maximise the initial benefits. The consumer can then decide how and with what device they will engage with for their on-going energy management. The open standard interface will ensure that there can be a number of providers who can compete in this space.

Additionally, we do not believe that account information should be displayed on the IHD as it would require additional security measures to be put in place which would drive up cost. There will also be situations where members of the household may need access to the IHD without requiring access to the account information (e.g. lodgers). The display of account information is a data privacy issue. The requirement to manage access to information extracted from the meter needs further analysis.

Q7	<i>Do you have any views or evidence relating to whether innovation could be hampered by requiring all displays to be capable of displaying the minimum information set for both fuels?</i>
We have no comment to make on this question at this stage.	

Q8	<i>Do you agree with the proposals covering the roles of and obligations on suppliers in relation to the IHD?</i>
<p>We agree with the recommendation that the supplier provides the base IHD with the installation of the smart meter. There is also the potential to allow consumers to have a creditor token towards a more sophisticated device; this would reduce the number of abandoned displays. There would need to be careful terms and conditions around the grounds for replacement to protect the supplier. There would need to be an obligation on the consumer to take reasonable care of the device and supplier to have to replace in the case of equipment failure rather than misuse or abuse. In the case of the pre-payment device the ownership of the device might be less clear to meet the requirements of the security required to maintain data integrity.</p> <p>The initial gains from the IHD are likely to be in the early adoption period when consumers start to understand the impact of their lifestyle and equipment usage. This will be translated into behaviour changes should they wish to save energy or money. The period of one year is likely to have these behaviours style either engrained or not adopted depending on the consumer. The benefits of the IHD after that period are therefore likely to be substantially lower so the value of keeping the IHD in order are less likely to be worthwhile so the period of</p>	

one year responsibility would seem reasonable.

### 3.7. Non-domestic Sector

**Q1** *Are there any technical circumstances where only advanced rather than smart metering would be technically feasible? How many smaller non-domestic customers have U16 or CT meters and what scope is there for full smart meter functionality to be added in these cases?*

To be addressed in our October response.

**Q2** *Do you agree with our proposed approach to exceptions in the smaller non-domestic sector?*

To be addressed in our October response.

**Q3** *Are there technical circumstances that we have not considered that would justify further flexibility around installation of either smart or advanced meters?*

To be addressed in our October response.

**Q4** *Do you agree with the proposed approach that use of DCC should be optional for non-domestic participants in the sector?*

To be addressed in our October response.

**Q5** *If use of DCC is not mandated for non-domestic customers, do you agree with the proposed approach as to how it offers its services and the controls around such offers?*

To be addressed in our October response.

**Q6** *To what extent does our proposed approach to the use of DCC for non-domestic customers present any significant potential limitations for smart grids?*

To be addressed in our October response.

**Q7** *Is a specific licence condition required to ensure that metering data for non-domestic customers can be provided to network operators or DCC, and should any provision be made for charging network operators for the costs of delivering such data?*

On the question that you are raising, we believe that it would be helpful to augment the existing Distribution and Use of System Agreement requirement with a licence obligation, and indeed wonder whether there is also a role here for the Smart Energy Code. The inter-relationship between the licences, agreements and Codes will be an important element of the arrangements. In addition we wonder whether this condition focuses more on charging arrangements for connectivity and usage, rather than metering data. The requirement for data to be provided free of charge implies more of a "from time to time" arrangement than will be the case when smart metering is rolled out. We also note the recommendation that the use of the DCC is not mandated for non-domestic customers given the existence of a current market - however the DCC will still potentially be seen as "dominant" due to the comparative scale of the consumer market. We therefore suggest that a licence provision should be made for the provision of metering data for non-domestic customers and that a charging mechanism should be established (which needs to be competitive with the existing market but regulated).

**Q8** *How can interoperability best be secured in the smaller non-domestic sector?*

To be addressed in our October response.

**Q9** *What steps are needed to ensure that customers can access their data, and should the level of data provision and the means through which it is provided to individual customers or premises be a matter for contract between the customer and the supplier or should minimum requirements be put in place?*

For smart metering to achieve its stated benefits for the non-domestic sector, we agree that customers should be able to obtain consumption information free of charge as with the

domestic sector at a useful level of detail and format, however the practicality for achieving this needs to be tested and any standards required to do so should be shaped by the industry. We believe that a centralised access control layer is required to secure the communications and data infrastructure for the non-domestic customers. Access control needs to be bi-directional to ensure that the industry has specific and role-based access to meter data while assuring that scheduled reads, alarms, configuration updates and real-time messages are sent to a valid, authenticated end-points which could be an ICT system (Information and Communication Technologies) for a non-domestic customer. Any access must follow the principle of "Defence in Depth" and include basic controls like firewalls and gateways, but should also include identification, authorisation, authentication and Public Key Infrastructure (PKI).

<b>Q10</b>	<i>Do you agree with our approach to data privacy and security for non-domestic customers?</i>
<p>More consideration is required for non-domestic customers as regards to the approach to data privacy and security. It is even more imperative that standards and interoperability agreements are established early in the smart metering lifecycle, as failures could have larger impacts on the system and customers due to the additional accumulation and association requirements of data collection. This in turn may require extra security enforcing functionality to protect the non-domestic customers. We recommend that, rather than an overarching high-level system approach, a separate threat, vulnerability, impact and risk assessment for non-domestic consumers needs be produced. This will enable a more pragmatic approach to security rather than enforcing any extra restrictive security enforcing functionality on to domestic customers. All risk assessments need be shared with suitable industry suppliers, as this will ensure that the "secure by design" principle and a common baseline is achieved. Once this is released, an industry-attended security working group would need to agree interoperability and security standards. This needs to be supported by the setup of a Security Governance Framework to ensure compliance and would furthermore need to be supported by an overarching Security Management Centre (SMC). The SMC would have ability to monitor; enforce and incident manage any issues or non-compliance on the smart metering system on behalf of the Security Governance Authority.</p>	

<b>Q11</b>	<i>Is the proposed approach to rollout (for example in terms of targets and a requirement for an installation code of practice) appropriate for the non-domestic sector?</i>
To be addressed in our October response.	

### 3.8. Regulatory and Commercial Framework

<b>Q1</b>	<i>Have we identified all of the key elements that you would expect to see as part of the Smart Metering Regulatory Regime?</i>
<p>We support in principle the broad regulatory regime proposed, particularly with respect to customer protection, certainty of delivery, competition and charging. We also agree with the key regulatory vehicles identified. We also suggest that adherence to standards/technical specifications and to service level agreements should also be explicitly covered within the regime.</p>	

<b>Q2</b>	<i>Do you agree with the proposal to establish a Smart Energy Code?</i>
<p>Yes. Smart metering is a new service, critical to the country and its infrastructure, the industry and most importantly consumers. A dedicated code is needed, embracing smart metering together with other key elements of effective energy management (certainly smart grid, possibly also smart homes and communities). In the interests of timescales, we suggest that the code initially focuses on smart metering and grid applications (to enable early establishment of the DCC) and is extended to smart homes and communities as soon afterwards as practicable as well as water in the longer term.</p> <p>We believe that close interworking between DECC/Ofgem on the one hand and Ofcom on the other will be required to deal with the substantial risks derived from the overlapping regulatory regimes applicable to the rollout of smart metering. We believe that some or all of the meter,</p>	

HAN, WAN and communications module fall within the definition of electronic communications apparatus for the purposes of the Electronic Communications Code ("ECC"). It also follows that the DCC is likely to be providing an electronic communications service and perhaps a network to its electricity industry customers and that therefore the basis on which it does so is subject to the provisions of the Electronic Communications Directives, especially the Framework Directive, the Authorisations Directive and the Universal Service Directive. Each of these instruments, which have been implemented in the UK by Regulations, contains provisions, especially restrictions, applicable to the imposition of regulatory obligations on providers of Electronic Communications Networks and Services. These will need careful review in the devising of the regulatory regime applicable to smart grids and smart meters.

**Q3** *Do you have any comments on the indicative table of contents for the Smart Energy Code as set out in Appendix 3?*

We have no comment to make on this question at this stage.

**Q4** *Do you have any comments on the most appropriate governance arrangements for the Smart Energy Code?*

We have no comment to make on this question at this stage.

**Q5** *Do you agree with the proposals concerning the roles and obligations of suppliers in relation to the WAN communications module?*

To be addressed in our October response.

**Q6** *We welcome views as to which other additional data items should be included in the mandated HAN data set beyond the list for the IHD.*

The data set should contain the minimum data for the minimal displays to work, the additional data that can be provided by the devices will act as a service and product differentiator. The open protocols that are most likely to be used will support that additional data as additional fields.

The "normal" bill units for gas and electricity units need to be consistent with those on the IHD so that the consumer can interpret information from both sources in the same way. The calorific value of the gas is relevant to the gas energy value and this information would need to be provided to the IHD in some way by the supplier.

If there was a method of reconciliation of the customer's retailer account data with the IHD so that the IHD actually displayed their rolling account this would reduce any variance. If this data could be passed from the retailer to the IHD even daily or weekly it would potentially increase the perceived accuracy of the billing as the consumer will consider the IHD as correct and any variance due to rounding errors of clock periods as mis-billing. The real time or update presentation of account information would need to be protected suitably to ensure security, and a methodology provided so only the account holder can see this information on the IHD and compliance with any data protection legislation is maintained.

The implied ability for a consumer's computer to directly access the stored data on the meter is a concern and would require more detailed requirements analysis.

We recommend that the starting position for the IHD is that it is not intended to be a means of validating the bill. The minimum data set should be so defined so as to facilitate competition at all levels of energy supply, and prevent consumer 'capture' by individual suppliers who hold exclusive information about individuals or groups of consumers.

**Q7** *Do you agree with the proposal that the WAN and the HAN in customer premises should be shared infrastructure, with the installing supplier retaining responsibility for ongoing maintenance? If not, would you prefer to have an arrangement by which if the gas supplier is the first to install, responsibilities for the common equipment is transferred to the electricity supplier when the electricity smart meter is installed?*

To be addressed in October response.

**Q8** *Are there additional measures that should be put in place to reduce the risks to the*

	<i>programme generated by early movers?</i>
<p>Key risks relating to early movers and our suggested measures to reduce them are:</p> <ol style="list-style-type: none"> <li>Early agreement of functional and technical specifications (covering meters and their communications) before permitting early mover rollout of smart meters;</li> <li>Comprehensive and early public and industry (including journalists and analysts) communications activities so as to clearly explain the smart metering programme and the positioning of early movers. It may be worthwhile extending this to local community events, celebrity champions etc.;</li> <li>Consider restricting early mover volumes to mitigate the risk of national optimum solutions being rendered economically unviable by an early 'dash' for the easy ones. We caution that there are numerous communications technologies that would offer suitable solutions for 60 or even 70% of the target premises. The real challenge is ensuring uniform service is available nationwide at a sensible cost, with the final 30-40% of premises being both technically and commercially challenging. An early 'dash' for the first 70% may well render uneconomic the remainder given these 'left overs' will not be geographically cohesive but will be intermingled among the 70% and likely require an alternative national infrastructure to address them. A national infrastructure is wholly affordable when amortised across the entire number of target premises, but becomes less viable as that number declines. It is for this reason that we caution that while volume early installations may feel supportive of programme acceleration, it runs the real risk of leading to an outcome whereby national deployment is never achieved;</li> <li>Hence we recommend that any meter deployment targets set for energy suppliers are kept low and based on industry process refinement objectives rather than meter installations;</li> <li>Define minimum datasets, upgradable APIs and technical standards as early as possible to prevent stranded installations and atomisation of the system.</li> </ol>	

<b>Q9</b>	<i>What is needed to help ensure commercial interoperability?</i>
<p>We suggest that commercial interoperability needs to have the following elements in place:</p> <ul style="list-style-type: none"> <li>standard charging types across both electricity and gas suppliers for minimum services;</li> <li>standard minimum terms and conditions;</li> <li>pre-agreed mechanism for offsetting/balancing costs incurred by the original installer at the point of shared use of the meter infrastructure (including communications and IHD) or transfer to another supplier;</li> <li>technical standards;</li> <li>common APIs.</li> </ul> <p>These elements need to be included within the supplier's licences, reflected in the Smart Energy Code and governed through DCC's licence. Commercial interoperability will be most easily achieved if the number of communications solutions and providers are minimised. A multi communications solutions environment with many complex technical and service interfaces will increase the challenge in achieving seamless commercial interoperability.</p>	

<b>Q10</b>	<i>Can current arrangements for delivering technical assurance be developed to gain cost effective technical assurance for the smart metering system? If so, how would these procedures be developed and governed?</i>
To be addressed in October response.	

<b>Q11</b>	<i>Are there any other regulatory and commercial issues that the programme should be addressing?</i>
<p>We understand that a review is taking place of the scope and responsibility of regulatory bodies. The communications services for smart metering will have a profound impact on the way in which in-home services are delivered, offering new ways of provisioning services to consumers. This scale of communications programme (connection to every domestic property in the country) should therefore be of strategic importance to Ofcom (as well as Ofgem) and we would therefore recommend that the appropriate Licence and code provisions are, as a</p>	

minimum, shared and agreed by both regulators.  
 We also recommend that, in the interests of timescales, early procurement activities are undertaken to place contracts with communications service providers, in parallel with the development of DCC Licence. We support the principle that the DCC should be separate from the communications service providers.

**Q12** *What evolution do you expect in the development of innovative time-of-use tariffs? Are there any barriers to their introduction that need to be addressed?*  
 We have no comment to make on this question.

**Q13** *Are there changes to settlement arrangements in the electricity or gas sectors that are needed to realise the benefits of smart metering?*  
 We have no comment to make on this question.

**Q14** *What arrangements would need to be put in place to ensure that customers located on independent networks have access to the same benefits of smart metering as all other customers?*  
 To be addressed in October response.

**Q15** *Are there any other industry processes that will be affected by smart metering and which the programme needs to take into account?*  
 To be addressed in October response.

### 3.9. Rollout Strategy

**Q1** *Do you believe that the proposed approach provides the right balance between supplier certainty and flexibility to ensure the successful rollout of smart meters? If not, how should this balance be addressed?*

The Prospectus is right to call for a mandated volume commitment roll out of smart meters post establishment of the DCC, and we fully support this. The mandated roll out will provide certainty to communications service providers to invest in solutions, and will deliver more efficient means of communication to achieve high degrees of service levels (such as first time installation success rate) whilst reducing the costs of the overall programme.

However, certainty for suppliers is not provided in the proposed staged implementation pre-DCC. It is only once the DCC is in place and has defined the enduring communications solutions that suppliers will be to procure meters with the appropriate specification and for those meters to be supported by the DCC.

Under the arrangements outlined in the Prospectus a common procurement date will be difficult to achieve as interim contracts are likely to have different terms (for instance volume commitments).

The Prospectus proposes two options under staged implementation, i.e. short term contracts or contracts capable of being novated. Neither are workable for the following reasons:

- In both cases Interoperability is required to ensure there is no need to exchange the meter asset, as this would introduce additional costs into the programme;
- As such it will be essential to establish pre-DCC technical and commercial interoperability;
- The staged implementation must assume interim interoperability is achieved, and the difference in communications costs is only £200m compared with full establishment. However this is not sufficient to allow for the duplication in systems which will be required;
- DECC's previous estimate in the December 2009 impact assessment was an additional capital spend of £760m for the systems for all the energy companies under

the fully competitive model;

- In the event interim interoperability is not achieved the £200m difference in the two models does not allow for replacement of the meters at the end of their short term contract period;
- Interim interoperability will need to consider all the enduring design requirements to mitigate any risk of consumer criticism;
- The introduction of new functionality to meters such as remote disconnect and the ability to remotely switch between pre-payment and credit, as well as the potential for smart grid functionality, increases the potential impact of security breaches, whilst the accessibility of public communications networks increases the likelihood of attempted attacks;
- Added to this threat will be the adoption of multiple open standard HAN protocols, increasing the risk of unauthorised access by 3<sup>rd</sup> parties to the HAN.

Without established technical and commercial interoperability, short term contracts will add complexity and cost to the Programme, as in effect the suppliers will be creating the competitive-led market model.

The single significant risk to the Programme is securing consumer confidence - if interoperability and security are not addressed as early as possible in the Programme additional costs and risks will be incurred.

We therefore recommend an alternative approach consisting of:

- defining programme and user requirements/objectives. Base requirements on end to end SLAs to reflect current and future requirements, ensuring that the limitations of current solutions are not adopted. Consider those SLAs really important to the success of the programme, such as an SLA for the connectivity to meters, rather than homes, an install success rate SLA for connecting and communicating with meters, SLAs for latency, etc.;
- issuing an OJEU notice that encapsulates the full potential scope of the communications service providers (including both secure communications and data management services);
- issuing an RFI for secure communications, and seek specification type responses from potential service providers [issue the RFI in Q1, 2011];
- using the procurement process through 2011 to narrow the options;
- awarding central communications contract with specification based on final solution [Q1, 2012].

Through this approach, technical specifications on other aspects of the Programme, such as meter specifications, can be developed in parallel with the communications service specifications such that the overall implementation timescales are not impacted.

This approach would lead to the following timescales:

Date	Milestone
End 2010	Define user requirements for end to end service
	Define system architecture
	Develop meter and communications specifications
Q1 2011	Issue RFI for central communications service provider
Q3 2011 to Q1 2012	Issue RFP, short list, negotiations Finalise meter specifications
Q2 2012	Award contract for central communications service provider and assign to DCC (DCC anticipated to be in place through an accelerated (alternative) DCC selection process)
Summer 2012	Mandated supplier rollout commences, as proposed by Prospectus, but adopting the enduring solution rather than interim pre-DCC solutions
Q2 2012 to Q2 2013	Enabling rollout from Q2, build, test and commission centralised

	communications service functions
--	----------------------------------

<b>Q2</b>	<i>Would the same approach be appropriate for the non-domestic sector as for the domestic sector?</i>
<p>The non-domestic sector will be an important part of the smart metering demand response solution for smart grid, as the non-domestic sector will be some of the largest consumers who potentially will provide the most flexible consumption patterns.</p> <p>For instance one of BT's locations has been selected for use in several LCNF bids as a significant consumer load on the local distribution network. Using a mix of battery back power solutions these non-domestic consumers can make a significant contribution to smoothing demand on the local distribution network.</p> <p>We therefore recommend a similar uniform approach for non-domestic premises, as these are likely to be used ahead of domestic premises.</p>	

<b>Q3</b>	<i>Is there a case for special arrangements for smaller suppliers?</i>
<p>We recognise that smaller suppliers, by definition, don't have the same purchasing power as large suppliers, and rolling out early is cost prohibitive in terms of negotiating carriage costs and development of and integration with head-end systems.</p> <p>Smaller suppliers should be encouraged to engage in smart meter rollout, however this requires a level playing field, where there is fair, reasonable, non-discriminatory access for all suppliers on equal terms. This is best achieved through an early procurement of an end to end centralised communications service provider providing the range of services which smaller suppliers cannot themselves provide and through establishing arrangements with ALL suppliers pre-DCC on terms that don't dissuade smaller suppliers, but actively encourage competition in the energy market.</p>	

<b>Q4</b>	<i>What is the best way to promote consumer engagement in smart metering? As part of broader efforts, do you believe that a national awareness campaign should be established for smart metering? If so, what do you believe should be its scope and what would be the best way to deliver it?</i>
<p>We support the use of a national awareness campaign, and have direct experience of the success of such campaigns through experience of programmes such as the Digital Switchover. However, we believe that local campaigns are also essential and this is demonstrated through the following example.</p> <p>PowerStream [1] an Ontario based utility company has rolled out smart metering to its 285,000 customers deploying on a regional basis, street by street. The consumer engagement programme was targeted on a local basis, using print media, local radio, as well as pre and post communications collateral.</p> <p>The consumer engagement campaign commenced on a utility wide basis. In the Ontario market model customers are first switched to a smart meter and then at a later date have their consumption data flowed to the Provincial Meter Data Management Repository. Once sufficient customer consumption data history has been established to provide full verification, validation and estimation functionality the consumer is switched to Time-of-Use (TOU) rates. This migration period is approximately 12 months in duration. Initially this proved somewhat frustrating to some customers who assumed that the installation of their smart meter also meant that they had been switched to TOU rates (those whom benefited from TOU rates). However, customers gradually became comfortable with the staggered implementation, especially after developing familiarity with the comparative bill information created by PowerStream to support their migration to TOU rates. The utility continues its regional roll out and communication approach, which enabled customer feedback to be better managed and adoption rates to be improved.</p> <p>PowerStream now fulfils on a regional deployment basis and then migrates the entire region to time of use tariffs following a cooling down period of at least a 12 month period. This</p>	

approach increases consumer advocacy and localises any consumer issues, and reduces the effect of a utility-wide challenge.

The migration period between meter installation and actual TOU rate implementation is used to highlight existing energy consumption patterns and offer advice to consumers to reduce their energy consumption or offer energy saving packages, such as insulation. When the TOU tariffs are finally implemented, the consumer is aware of the necessary measures required to reduce energy consumption.

**[1] Source: Direct comment from PowerStream**

**Q5** *How should a code of practice on providing customer information and support be developed and what mechanisms should be in place for updating it over time?*

We agree with the recommendation that there should be a code of practice for customer information to ensure that a common standard is achieved. Suppliers may provide additional information over and above the minimum level, providing that it does not contravene the code of practice relating to supplier installation visits (i.e. unwelcome selling). We suggest that the suppliers be obligated to report on the delivery of such information (e.g. % of consumer installs for which information was not supplied) and also on consumer feedback as to the content provided. Consumer feedback should then be aggregated by Ofgem on an annual basis to determine whether any changes to the code of practice are required or indeed any improvements in supplier performance (e.g. clarity of information provided) are needed.

**Q6** *Do you agree with the proposed obligation on suppliers to take all reasonable steps to install smart meters for their customers? How should a completed installation be defined?*

All consumers have right to have a smart meter. No consumer should be disadvantaged by not being able to connect their gas, electricity or water meter to the central communications provider network. Therefore the communications solution should be designed to connect to 100% of meter locations in GB. Gas and water meters should not have to rely on a HAN, where there is no service level assurance.

Completed installation is defined by:

- the relevant meter (electricity, gas, and where appropriate water) is installed, commissioned and communicating to the WAN head-end;
- the accredited IHD is installed and operating for the utility/utilities being installed. If the programme was to be extended to include water, then there should be an option to allow water consumption and related data to be included on the IHD.

**Q7** *Do you think that there is a need for interim targets and, if so, at what frequency should they be set?*

We support the introduction of interim committed volume deployment targets, post establishment of the DCC. We recommend the targets are published ahead of the procurement of the centralised communication provider and start once the central communications provider has been procured.

The interim committed volume deployment targets will provide a greater degree of certainty. This will allow bidders for communications service provider to investment in alternative communications solutions which deliver more efficient mechanisms for roll out, such as improved first installation success rates, reducing the overall costs of the programme.

Rolling 12 month volume deployment targets should provide sufficient certainty for internal capacity forecasting (manufacturing and logistics) and for the communications infrastructure build. The volume targets will also allow the creation of a more accurate cost profile, giving more certainty over price.

Targets should be set through the life of the Programme to ensure suppliers provide all consumers the option of a smart meter. It might be helpful to align early interim targets to encourage coordination between suppliers, possibly by defining geographies to focus on, to

facilitate accelerated rollout.

The benefit of this approach would be to increase certainty for the DCC over the timing of establishing and sizing the end to end solution.

Increasing the volume commitments in the first four years to achieve >90% of meter installs, will provide greater certainty on capital investment, reducing the cost of project capital which will have a knock on effect to price.

The risks associated with bringing forward the roll out commitments are related to the first time installation success. If the first time installation success is low, the costs of revisits will escalate closer to the target date.

**Q8** *Do you have any views on the form these targets should take and whether they should apply to all suppliers?*

We agree with the general approach suggested in the Prospectus. This provides DCC and the central communications provider with a baseline of growth with which to match its services, specifically scaling of its end to end solution architecture.

In answer to other questions in this response, we have proposed that the DCC and the central communications provider be appointed in time for the mandated interim rollout targets. This means that the interim rollout can be implemented with the enduring communications solution from the outset.

In addition, we would propose targets be applied by DCC to the central communications provider. Such targets should include:

Target
Coverage target (indoor meter connectivity)
90% within defined geographic rollout regions within 12 months
80% of GB-wide existing meter locations within 18 months
>99% of GB-wide existing meter locations within 3 years
First time meter install success rate of >95% within coverage areas

The coverage target is critical as without it solutions may be adopted that don't support the rollout of meters to every home.

**Q9** *What rate of installation of smart meters is achievable and what implications would this have?*

From a perspective of a professional communications company, we recommend the communications solution should be chosen to deliver the highest Net Install Success Rate. This will ensure focus is on new installs rather than revisits.

	Current smart metering cellular trials	The proposed industry requirement
WAN indoor geographic coverage to meters within 2 to 3 years	70% [1]	99%
1 <sup>st</sup> time install success rate (excludes property access rate)	80%	95%
Calculated Net Install Success Rate	56%	94%

[1] Source: Accenture, high-level assessment of smart meter technology in the UK, 2008. Cited within Carbon Connections: Quantifying mobile's role in tackling climate change, July 2009, Vodafone

This clearly demonstrates the necessity for a high degree of installation success.

From the table above, that the differential between Net Install Success Rates is 94% versus 56%. Under current smart metering solutions, around 3 in every 5 homes targeted with a smart meter installation will fail. It is therefore imperative to procure a central communications

WAN solution that achieves the highest coverage and installation success rate.

The improved efficiency shown in the table (94% Net Install Success Rate versus 56%) will result in

- an accelerated meter rollout (less time spend on revisits or abandonment)
- improved customer experience (less revisits)
- efficiency savings of £hundreds of millions (analysis provided separately)

The rate of installation is affected by the meter install success rate (needs to be a mandated KPI and be equally applicable for electricity, gas and as applicable water meters). Therefore we recommend the Programme procure a communications solution that will deliver the highest success rate.

The Net Install Success Rate and accelerated rollout can be maximised by

- enabling, as an option, the gas meter to connect directly to the WAN where there is no HAN connectivity
- co-ordination of rollout by geography, with focus on the major population areas first
- connecting the water meter to the WAN
- mandating a KPI for meter connectivity as a target for the central communications service provider
- an efficient meter communications commissioning process.

**Q10** *Do you have any evidence to show that there are benefits or challenges in prioritising particular consumer groups or meter types?*

We have no evidence relating to particular consumer groups. However, we believe that communicating direct to the meter via the WAN will enable any meter to be installed in any order, including water meters. This would allow for a more flexible rollout allowing gas and/or water installations to proceed ahead of the rollout of electricity smart meters if so desired.

We believe there is merit also in co-ordinating the supplier rollouts around certain geographical areas. By targeting a specific region or city, the local awareness of the rollout will be heightened which should lead to improvements in access rates. This should also allow more economical rollout to be achieved through co-ordination.

**Q11** *Do you agree with our proposed approach to requiring suppliers to report on progress with the smart meter rollout? What information should suppliers be obliged to report and how frequently?*

We agree that suppliers should report on progress of smart meter rollout. We would expand this requirement to the central communications provider who, reporting through the DCC, should report on rollout and network performance for the meters connected to the network. This will reconcile what is installed versus the meters being served by the DCC.

In addition to the reporting requirements listed, we propose the following information will help all stakeholders understand the success of the programme:

Report on	Who	Frequency	Benefit
Coverage areas (indoor/outdoor) by postcode where near 100% connectivity of meters is available	Central communications service provider via the DCC	Monthly	Helps with coordination of meter rollout, consumer awareness programme and meeting of SLAs
Quantity of meters installed, by geographic area per technology	Suppliers	Annually	Demonstrates progress against programme
Homes connected within coverage areas	Central communications service provider via the DCC	Monthly	Reconciles and demonstrates progress to mandated targets

	+ suppliers		
Breakdown and mix of electricity, gas and water meter connected	Central communications service provider via the DCC	Monthly	Demonstrates progress against programmes
Network availability percentage	Central communications service provider via the DCC	Monthly	Demonstrates progress against SLAs
Install success rate (following property access)	Suppliers	6-monthly	Demonstrates progress against SLAs
Communications failures requiring revisits	Suppliers	Annually	Demonstrates progress against SLAs

<b>Q12</b>	<i>Do you agree that there is already adequate protection in place dealing with onsite security or are there specific aspects that are not adequately addressed?</i>
We believe that existing codes of practice for consumer visits (such as ERA's) are adequate for their current purpose but need extending for the communications activities and physical works required for smart metering.	

<b>Q13</b>	<i>Do you agree with our proposal to require suppliers to develop a code of practice around the installation process? Are there any other aspects that should be included in this code of practice?</i>
<p>The proposal within the Prospectus to include a code of practice for the installation of meters is vitally important to maintain customer confidence in the Programme. The DCC should also have a commitment to publish the results of the KPIs associated with the installation success given this programme is funded through the consumer.</p> <p>The code of practice should include procedures to measure the success of the installation. This includes all aspects of the equipment, meters, IHD, HAN and WAN connectivity. This information will help inform the DCC, the regulator, and Government measure the success, by monitoring the performance of the code. The data can be used to quickly identify any divergence from the cost targets attributed to an increased rate of abortive or failed installations not conforming to the code of practice.</p> <p>Unless the code is measured and monitored it is doubtful whether it would provide any significant value to the programme.</p> <p>The code of practice should include an ombudsman to resolve any disputes that may occur between the consumer and the supplier.</p> <p>The supplier should be made to publish a separate complaints process for the installation as part of the code of practice.</p> <p>As part of the reasonable endeavours commitment, suppliers should ensure the agent has suitable access to the central communications provider to resolve any onsite issues first time.</p> <p>It is agreed that an independent audit should be carried out using a sample poll of target consumers, and the results of this poll should be open to public scrutiny. We agree that this should help build consumer confidence.</p>	

### 3.10.Statement of Design Requirements

<b>Q1</b>	<i>Should the HAN hardware be exchangeable without the need to exchange the meter?</i>
The wireless technologies and protocols that are used within the home are likely to move forward at a much faster pace than the WAN protocols and evolution is likely to be faster than	

the 15 year expected life of the meter itself. Therefore, it would be sensible that the HAN "card" within the meter be able to be replaced by an engineer with minimal work. In order for there to be flexibility for manufacturers and to promote competition the interface between the meter and the HAN card would need to be an agreed standard interface with published interface specification.

If the HAN is not used for any critical operations, e.g. gas meter reading and valve operation then it may be possible for the HAN interface card to be external to the sealed part of the meter. This may lead to the possibility of an external plug in, such as serial, USB or other published interface for the HAN module to be communicated with and be powered from. This would free the HAN interface card from the regulated side of the electricity supply and be user or user agent interchangeable without loss of critical supply control. This would also have the benefit of the HAN unit being able to be replaced or repaired by a third party on non meter accredited engineer. This might address a key issue with replacing the HAN hardware, which is that the cost of deploying engineers to every meter address more frequently than the current meter service life requires, results in retailers or their agents incurring significant additional costs.

This may have an impact for demand management within the home but if this was lost due to the consumer replacing or removing the HAN then they could fall back to a tariff that did not have the benefit of demand management of micro generation input.

In summary, a field changeable HAN module is seen as desirable but the methodology for the change process needs consideration.

**Q2** *Are suitable HAN technologies available that meet the functional requirements?*

At present there is no HAN technology that can deliver all the functional requirements in a secure and open way. There is work going on within this technology arena that meets a substantial number of the functional requirements. It is our view that mandating an open standard may not be the best way to achieve all the functionality required, and that it would be better to allow the suppliers to choose a standard that best fits the technical needs of the solution within a competitive framework.

**Q3** *How can the costs of switching between different mobile networks be minimised particularly in relation to the use of SIM cards and avoiding the need change out SIMs?*

We see a number of issues with switching between different mobile networks:

- Unless a roaming mechanism is utilised, the Supplier's installer will need to have a variety of SIM cards for different networks in order to select one which will connect to the meter in its location in the home;
- If roaming is utilised, then care needs to be taken that this does not extend to networks that may not meet the national security requirements required for smart metering;
- Mobile networks by design are used for multiple purposes and are therefore subject to frequent changes. These may impact the effectiveness of the connectivity to the installed meter and may require a re-visit to swap out the SIM card to utilise the changed network or to select an alternative network. In turn this adds further cost to the Programme;
- Mobile coverage varies considerably between networks and choices may not therefore be available;
- Costs would be minimised by placing a long term contract (benchmarked for value for money) rather than multiple short term cellular contracts.

**Q4** *Do you believe that the Catalogue is complete and at the required level of detail to develop the technical specification?*

This answer builds on the answer provided for Prospectus Q6 above regarding the Functional Requirements.

The Catalogue should specifically address the need to allow for an early rollout based on WAN communications integrated into the electricity, gas and water smart meters with a forward compatible approach to avoid the risk of stranded assets.

It is recommended that more information should be provided at the earliest possible stage on the required SLAs including the need for longevity, security and data integrity in processing data and commands from electricity, gas and water smart meters. SLAs should also be specified within the catalogue for first time successful installation and the number of revisits required in the 15 year life span of the smart meters.

To improve data integrity it should be allowable for data from a particular smart metering System to be relayed to the WAN by a neighbouring smart metering system. The data integrity and security in this instance must be maintained via tight access control, encryption, and cyber intrusion management.

There should be a functional requirement to provide real time meter readings to supplier call centres automatically on customer queries within 30 seconds. This would be of negligible cost but would provide the benefit of improvement in customer service.

HA.11 suggests that gas meter consumption information should be delivered to the IHD every 30 minutes but IH.2 states 15 minutes for the same requirement. For the balance of consumer information and preserving battery life, an update of 30 minutes seems reasonable.

Q5	<i>Do you agree that the additional functionalities beyond the high-level list of functional requirements are justified on a cost benefit basis?</i>
Q6	<i>Is there additional or new evidence that should cause those functional requirements that have been included or omitted to be further considered?</i>

**The table below answers both question 5 and 6.**

<b>Additional functionality</b>	<b>Accepted/ Rejected Category</b>	<b>Response Comment</b>
Diagnostic Logs	Accepted	Agree
Tariff Structures	Accepted	Agree
Prepayment	Accepted	Agree
Data for planning purposes	Accepted	Agree
Other meters and equipment	Accepted	Gas and water meters are better served with direct WAN communication integrated to the meter. This allows flexibility to roll out gas and water smart meters independently and allows for clarity on SLAs and maintenance responsibility independent of the HAN
Last gasp communications	Accepted	Agree. Benefit: Local level fault isolation e.g. between the last transformer and the home. Suggest KPI of 90% report success against 2,500 homes is achievable.
Ability to exchange WAN module	Accepted	The WAN should be integral to the meter and be certified for the full 15 year life of the meter
Temperature Sensing	Rejected	Agree
Auxiliary switches	Rejected	Demand response programs will be better served with auxiliary switches rather than Load Control Modules connected via the HAN
Pulse output	Rejected	Agree

Q7	<i>Do you agree that the proposed approach to developing technical specifications will</i>
----	--

<i>deliver the necessary technical certainty and interoperability?</i>	
<p>There is a definite risk that the proposed approach will not deliver the necessary certainty and interoperability. This is because the programme is trying to deliver a specification to cover all possible solutions including multiple HANs and multiple WAN technologies, as well as a fully competitive communications model, which inevitably increases complexity and risk in terms of technical and commercial interoperability.</p> <p>A preferred approach would be to start the specification and procurement process earlier through an immediate RFI, to help create/inform/ratify the technical specification, drawing on industry experts in their field.</p>	

<i>Q8</i>	<i>Do you agree it is necessary for the programme to facilitate and provide leadership through the specification development process? Is there a need for an obligation on suppliers to co-operate with this process?</i>
<p>The programme should focus on the RFI/RFP process to establish the requirements for the WAN provider as soon as possible. Suppliers should be obliged to cooperate in drafting the requirements and should be obliged to comply with the result of the procurement process.</p>	

<i>Q9</i>	<i>Are there any particular technical issues (e.g. associated with the HAN) that could add delay to the timescales?</i>
<p>From a communications perspective, potential technical issues that need to be managed include:</p> <ul style="list-style-type: none"> <li>• Selection of a HAN technology that performs to a minimum expected range and with appropriate building penetration characteristics (specific KPIs should be defined to help with the selection of HAN technology). This is particularly important for meters that are not co-located;</li> <li>• Irrespective of the HAN and WAN technology, we propose there needs to be clear accountability for the performance of connectivity to meters, including the HAN if this is used;</li> <li>• Provide for the option of connecting meters directly to the WAN (in case HAN connectivity is not possible). Establish KPIs for the performance of the WAN with the central communications provider;</li> <li>• The IHDs may have a range limitation within the home. Expectations need to be clear with consumers to avoid disappointment;</li> <li>• Specifications for customer premises equipment need to be developed in parallel to defining the end to end solution and selecting the WAN technology. Within this response, we propose a parallel procurement of the central communications provider. This approach will help to avoid technical issues due to inter-dependencies between different elements of the end to end enduring solution;</li> <li>• We recommend against the adoption of multiple HAN and WAN technologies, security solutions, head-ends and central data. This will only complicate and amplify the range of technical issues that could be encountered, making resolution of issues more complex;</li> <li>• Procure a single central communications solution provider who will integrate and manage the end to end technical risk and will act as single point of accountability for the performance of the communications solution.</li> </ul>	

<i>Q10</i>	<i>Are there steps that could be taken which would enable the functional requirements and technical specifications to be agreed more quickly than the plan currently assumes?</i>
<p>We fully support the work on developing technical specifications for the meters and recommend the programme works in parallel on other aspects of the end to end solution, such as the IHD, HAN, WAN and central services. Finalising specifications for the meters will be extremely helpful but there are interdependencies between various solution elements that we believe need to be considered in parallel.</p> <ul style="list-style-type: none"> <li>• Until the WAN is selected, it is impossible to complete the technical specifications for the meters, the communications hub, the IHD or the central services. The communications provider must be responsible, through SLAs, for the performance of</li> </ul>	

the connectivity to the meters. For instance, should connectivity to the meters be via the HAN or direct to the WAN?;

- The end to end risks to be managed by the central communications provider need to be defined;
- Responsibility for the performance of the HAN needs to be defined;
- Only when there is an understanding and agreement of an end-to-end solution architecture should decisions be made as to where data and functionality should reside, i.e. within the central communications services, within the communications hub or within the meter. Such decisions should also take into account the associated costs.

Specification of other elements of the end to end solution therefore needs to be developed to keep pace with and influence the final meter specifications.

We recommend a re-ordering of the Programmes activities to address these issues.

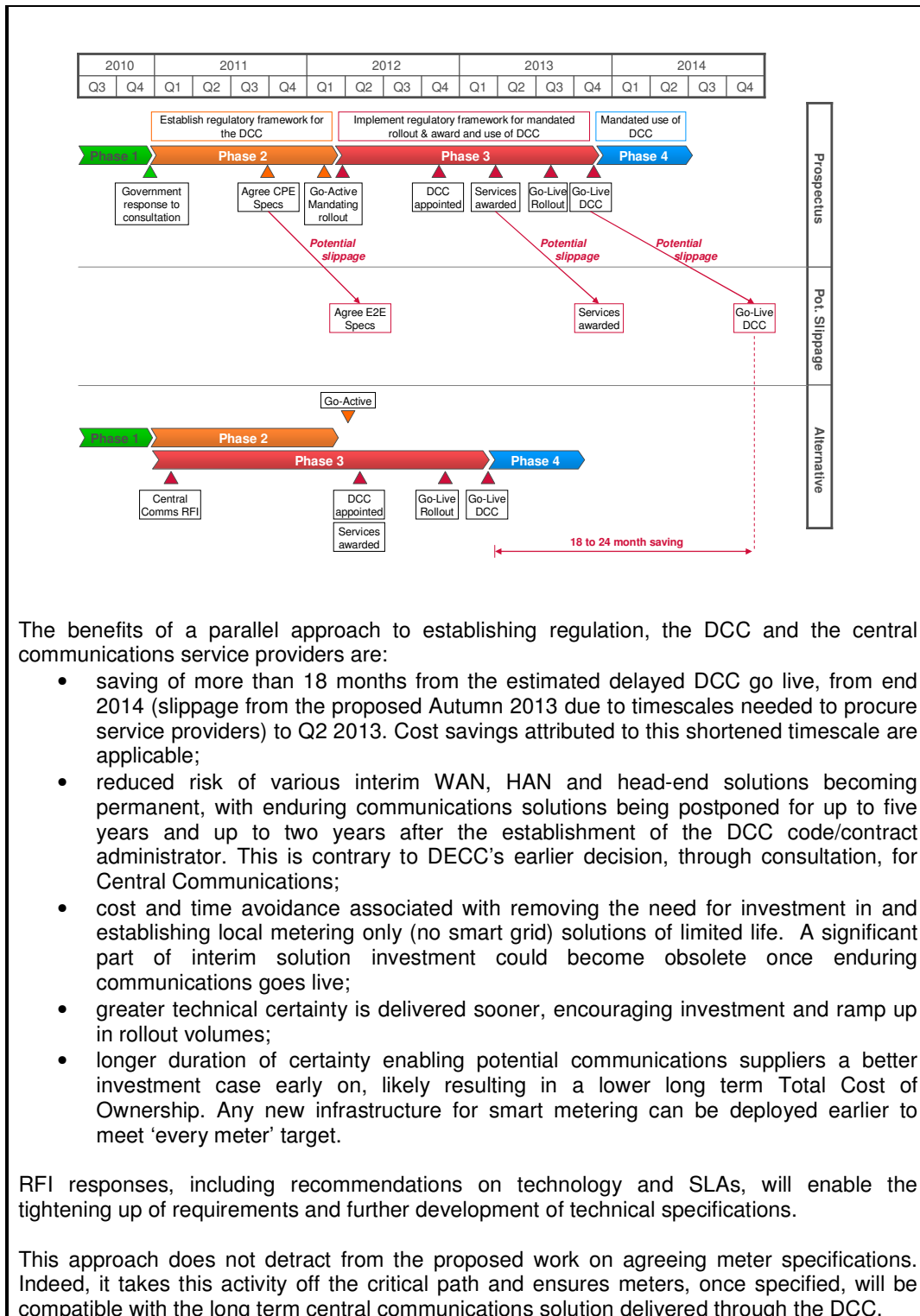
- defining programme and user requirements/objectives. Base requirements on end to end SLAs to reflect current and future requirements, ensuring that the limitations of current solutions are not adopted. Consider those SLAs really important to the success of the programme, such as an SLA for the connectivity to meters, rather than homes, an install success rate SLA for connecting and communicating with meters, SLAs for latency, etc.;
- issuing an OJEU notice that encapsulates the full potential scope of the communications service providers (including both secure communications and data management services);
- issuing an RFI for secure communications, and seek specification type responses from potential service providers [issue the RFI in Q1, 2011];
- using the procurement process through 2011 to narrow the options;
- awarding central communications contract with specification based on final solution [Q1, 2012].

Through this approach, technical specifications on other aspects of the Programme, such as meter specifications, can be developed in parallel with the communications service specifications such that the overall implementation timescales are not impacted.

This approach would lead to the following timescales:

Date	Milestone
End 2010	Define user requirements for end to end service
	Define system architecture
	Develop meter and communications specifications
Q1 2011	Issue RFI for central communications service provider
Q3 2011 to Q1 2012	Issue RFP, short list, negotiations Finalise meter specifications
Q2 2012	Award contract for central communications service provider and assign to DCC (DCC anticipated to be in place through an accelerated (alternative) DCC selection process)
Summer 2012	Mandated supplier rollout commences, as proposed by Prospectus, but adopting the enduring solution rather than interim pre-DCC solutions
Q2 2012 to Q2 2013	Enabling rollout from Q2, build, test and commission centralised communications service functions

This is illustrated by the following:



The benefits of a parallel approach to establishing regulation, the DCC and the central communications service providers are:

- saving of more than 18 months from the estimated delayed DCC go live, from end 2014 (slippage from the proposed Autumn 2013 due to timescales needed to procure service providers) to Q2 2013. Cost savings attributed to this shortened timescale are applicable;
- reduced risk of various interim WAN, HAN and head-end solutions becoming permanent, with enduring communications solutions being postponed for up to five years and up to two years after the establishment of the DCC code/contract administrator. This is contrary to DECC's earlier decision, through consultation, for Central Communications;
- cost and time avoidance associated with removing the need for investment in and establishing local metering only (no smart grid) solutions of limited life. A significant part of interim solution investment could become obsolete once enduring communications goes live;
- greater technical certainty is delivered sooner, encouraging investment and ramp up in rollout volumes;
- longer duration of certainty enabling potential communications suppliers a better investment case early on, likely resulting in a lower long term Total Cost of Ownership. Any new infrastructure for smart metering can be deployed earlier to meet 'every meter' target.

RFI responses, including recommendations on technology and SLAs, will enable the tightening up of requirements and further development of technical specifications.

This approach does not detract from the proposed work on agreeing meter specifications. Indeed, it takes this activity off the critical path and ensures meters, once specified, will be compatible with the long term central communications solution delivered through the DCC.

- End of document -