Incident Management:
Q11 Do you agree with our proposed text for the SEC, with respect to Incident Management?

These comments are subject to the drafting of the Incident Management Policy, which awaits completion

Whilst we are in general support of the concepts of Incident Management outlined within the relevant, redrafted sections of the SEC, we do have further comments for consideration. These comments are subject to the completed drafting of the Incident Management Policy, which has not yet been written. However, we anticipate that the Incident Management Policy should conform to Information Technology Infrastructure Library (ITIL) as a minimum (see ITIL references within the Security section).

The SEC Section H9.1 includes the reference to the defined term Incident Category, the definition of which points back to section 9.1, thus forming a circular reference that does not define the term. We therefore ask that the definitions of Incident Category are properly established and clearly drafted.

The definition and development of Incident Categories 1 - 5 has been the subject of debate during several Commercial Working Group meetings, none of which have clarified how these have been defined. The CSP schedule [4.2] categorises the severity of these incidents based on the opinion of the DCC of a list of potential high-level impacts. The concepts outlined include the number of meters affected - the greater the number of meters impacted the greater the severity of the incident. However, in order to provide useful and meaningful incident management for the DCC Users who are paying for these services further consideration must be given to not only the number of meter-point outrages but also the type of fault and meter - point affected. For example, 20,000 meter-point outages would need to be dealt with differently if they were all prepayment customers. We ask that further consideration is given to how these categories are developed and that this is done in an open and transparent way, with the end – user in mind and involved. As a minimum, these assessments must consider industry processes, customers, types of meters impacted and cash-flows.

The drafting of the SEC needs to at least reference the CSP Schedule that deals with Incident Management to ensure clarity and consistency, once these have been properly defined.

We support the approach to conduct a major incident review, as outlined in H9.11, in order to capture lessons learnt and further improve incident management going forward. However, we believe that two days to undertake such a review and draft a detailed report of the findings to the panel in-line with a minimum set of requirements as defined in this section will be challenging. If insufficient time is given to this process the detail and quality of the assessment could be compromised, we therefore ask that consideration is given to a more appropriate time-scale for the work but that the drafting ensures that this assessment must start within two days of the resolution of the incident. Further, references to 9.13 should read 9.12.

Self-Service Interface:
Q12 Do you agree with our proposed text for the SEC, with respect to the Self-Service Interface?

We support the proposals to develop the Self-Service Interface and that the systems and processes developed to support this interface are to comply with ITIL standards. We do however have further comments for clarification.

General comments
The SEC consultation, paragraph 251, makes provision for the DCC to provide technical access credentials to the DCC Service Users, in order to determine the eligibility requirements for Self-Service Interface (SSI) use. These will include password requirements and minimum browser specifications.

Whilst we are in support of the approach being developed by the DCC to ensure controlled access to the SSI, we ask that consideration is given to the potentially wide range of legitimate access requirements that may exist. This may necessitate the need to develop systems and processes with an element of flexibility in mind and with suitable access controls being placed at an appropriate stage(s) within these processes, rather than restrictions being placed as a consequence of only allowing a limited number of technological platforms.

We support the obligation on the DCC to provide, maintain and keep an up-to-date central Incident Management Log but require further clarification as to how this log is intended to be managed. Paragraph 225 states that an incident that will have been raised by a DCC Service User will then be allocated to a DCC Service User for investigation. We do not see that it is appropriate for incidents to be managed by a DCC Service User but would have rather expected that it would be the responsibility of the DCC to investigate, manage and resolve most if not all of the incidents that may arise. We therefore seek clarification around this drafting and the DCC's intent in this regard.

Further, whilst we understand that it is the DCC's intent to establish the SSI as the primary source of information, consideration must also be given (particularly during the early stages of the Programme) that Users may need additional support whilst newly developed systems and processes and understanding develops. We therefore believe that it will be prudent not to strictly adhere to clause H8.12, during this period.

Specific comments
H8.15 The Self-Service Interface must (as a minimum) allow the following categories of User to access the following:

> (b) a record of the Service Requests and Signed Pre-Commands sent by **each** User, and of the Acknowledgements, Pre-Commands, Service Responses and Alerts received by that User (as a minimum during the preceding three months), which shall be available only to that User;

For the avoidance of doubt the above should be drafted to ensure that this clause only allows access to the specific User's communications with the DCC and not every User, in order to avoid any confusion. We await the detail that we anticipate will be contained within the Self-Service interface specification document when it is drafted for additional clarity.

DCC Service Desk:
Q13 Do you agree with our proposed text for the SEC, with respect to the DCC Service Desk?

We support the development of a Service Desk.

The SEC Stage 2 consultation, paragraph 254 states that the DCC Service Desk will form the primary communications channel for SEC Parties who are not DCC Service Users. We assume that this is a provision for independent energy companies wishing to service their customers independently and therefore requiring their opting-out of DCC Services. Whilst we understand that this is a requirement as this User group will, by default, not be eligible to complete the User Entry Processes required to access DCC information via the Self-Service Interface (SSI), we would like further clarity as to the information or services that the DCC envisages that these Users will require, if they are not using DCC Services. We do not understand what general queries this group of Users is likely to want to raise.

H8.13 – suggests that service desk contacts can be made by SEC parties who are not DCC Users. We are not sure of the scenarios envisaged here and so would ask for further clarity to be provided. If this approach is to endure then we ask that appropriate restrictions are considered for these forms of access.

Service Level Agreements for Testing:
Q14 Do you agree with our proposed text for the SEC, with respect to the Service Level Agreements for Testing?

We support the need to develop a DCC Service Level performance framework, but have some further points of clarification.

We do not support minimum service levels of 85% for Category 1 and 2 incidents

Firstly, we need to understand what testing is envisaged here as we can find no references in the associated sections of either the Consultation document or the SEC Legal drafting in terms of testing Service Level Agreements.

Whilst we understand the approach outlined in consultation paragraph 266 regarding DCC Service Level Performance, we still remain to be convinced that this approach is an improvement over that detailed in the now deleted section K9.6 and detailed within the calculation in K10.8. New service credits passed on to service users within future charging statements does not appear to be a benefit in terms of an earlier provision of any refund and the approach, as currently defined, appears to be less transparent.

Those parties that are responsible for paying the invoices associated with these methodologies require the ability to be able to forecast their effect and so make appropriate internal provision for payment. Further, it is feasible that a CSP issue affecting DCC performance levels could disproportionately affect a Supplier in a geographic area therefore they would not be sufficiently compensated for the loss of service if the reduction is smeared. We therefore ask that further information or clarification is provided in order to better understand this new approach and the reasons behind the proposed change for Stage 2.

As Category 1 incidents in particular can potentially have a large impact for both consumers and suppliers, we do not believe that setting a minimum Service Level target of 85% is appropriate and would expect a level of 95+% to be more appropriate in these circumstances. We ask that further consideration is given to the table as set out in paragraph 262 of the Consultation document to ensure that the levels summarised are acceptable to all.

Service Level Agreements for Testing:
Q15 Does the inclusion of DCC aggregate performance measures in the SEC, and the consequential reduction in future service charges, appropriately balance the need for the DCC to manage its Service Providers flexibly with the need for DCC Service Users to have a say regarding performance targets?

We are in general support of the proposed approach, but would ask that this is continually monitored during early stages of roll-out.

We are in general agreement with the proposed approach and support the timely and transparent report structure that is envisaged. As this is further underpinned by an inclusive stakeholder change control process we envisage that any unforeseen issues arising will be identified and dealt with effectively and efficiently.

By requiring the DCC to provide continuous plans and reports on all Service Level Performance measures that it is responsible for, in the same way that Suppliers are expected to do for their involvement in Smart Meter Roll-out, will further inform as to the context of the smart meter roll-out. The information provided by the DCC is both supplementary and complementary to these supplier reports and may help to provide contextual information as to the progress or otherwise of roll-out progress. Further, we would like to see appropriate penalties to be placed were failed service levels impact DCC Service Users adversely.

Such an approach will also facilitate a more effective and efficient stakeholder consultation process where service level threshold adjustments are required, as stakeholders will be more informed as to the prevailing issues. We assume that Suppliers, as ultimate end Users, will be stakeholders in terms of DCC adjustments to Service Providers' performance measures, we would seek clarification for any departure from this view.

SEC Consultation, paragraph 264 – we understand the need for the DCC to be able to be flexible with regard to managing its Service Providers. We ask that in order to ensure that the correct balance is struck with regard to managing detailed and aggregate service level changes that the change control process is monitored closely to begin with and provision made to readily amending that process if required. For example, aggregate performance measures should not be managed and reported at the expense of monitoring detailed performance measures by individual users. We believe that further, practical experience in this area will better inform the success, or otherwise, of the underlying processes employed to manage these changes. A form of continual improvement therefore would seem to be a practical way forward.

With regard to the DCC Performance Measures provided within the Consultation document itself we cannot approve the minimum service level of 85% being set for category 1 and 2 incidents without first reviewing any supporting information that was used to set the level at this value. These incidents by their nature will have large impacts on consumers and suppliers. We ask that this Service Level is reassessed and set to a more realistic level, for example, 95%. Failure in this area should have associated liquidated damages set at levels to appropriately reimburse affected consumers and suppliers.

Further, we would like to better understand the balance of incentives and penalties that are envisaged to assure ourselves that the aggregate measures suggested do not encourage perverse behaviour or provide overall measures that mask poor performance.

Managing Demand:
Q16 Do you agree with our proposed text for the SEC with respect to Managing Demand?

We disagree with the proposed text

The drafting of SEC Section H3.38 – H3.43 is based around a Demand Management Model whereby each User is required to regularly submit forecasts of the number of Service Requests that they will send going forwards, and the DCC then:

- monitoring how accurate these forecasts are, and where any individual User's forecast is exceeded by greater than or equal to 110% then the identity of each such User and the number of service requests sent by each such User is to be published on the SEC website.
- the DCC not being considered to be in breach of SEC with regard to its obligation to achieve Target Response Times, if, during the month in question, the aggregate Service Requests sent by all Users exceeds 110% of the aggregate demand most recently forecast for that month by all Users.

We have a number of concerns with this proposed model, and as such are not supportive of the legal drafting being proposed. Our concerns are detailed below:

Ability to Forecast Demand
The model is based upon an assumption that Users will always be able to forecast the number of Service Requests that they will send going forwards. This is not always the case however, as external factors that are outside Users' control, such as the Government declaring a change to VAT rate, can have a significant impact upon the volumes of Service Requests that Users will need to send going forwards, and we are not able to forecast for these external events. In particular, it is also very difficult to predict the demand for, and frequency of firmware updates – particularly in the early period after DCC go-live. Given the complexity of the end to end systems, this is not an improbable scenario and one which may consume significant bandwidth.

Sanctions
It is inappropriate to propose sanctions against Suppliers utilising a process which contributes to the stability of the network and the integrity of the market. In particular, publication of the latest forecast and the number of Service Requests on the SEC website may reveal commercially sensitive information.

Capacity Management
Central to the efficient management of any network is the capability to offer capacity in both operational and planning (strategic) timescales. This fact needs to be taken account of within the Demand Management Model and the drafting of SEC Section H3.38 – H3.43.

Sharing of operational capacity allocations
In operational timescales, it may be appropriate to manage the phasing of user requests in order that a 'peak' is avoided. Consequently, dividing up an annual

capacity allocation into equal fixed monthly, precludes User X utilising User Y's capacity when it is able to do so. We believe that there would be benefit in considering more flexible options such as the implementation of a "capacity sharing" approach, whereby if User X has spare capacity the DCC should be able to re-allocate this to User Y according to some principles around 'fair use'.

Managing operational capacity through message prioritisation

Clause H3.42 states that the DCC should submit a Modification Proposal containing appropriate rules to enable the prioritisation by the DCC of Service Requests, Service Responses and Commands, in circumstances where the aggregate demand for the same cannot be simultaneously satisfied. This is another "peak congestion management technique" that we trust would be reserved for exceptional circumstances. Any prioritisation regime will have significant commercial implications dependent on both the role of the User and the purpose of the message.

Release of efficient new capacity

We are concerned that there appears to be no mention of a mechanism by which the DCC can consider building additional capacity in response to meeting Users' demands. This may, in the long term, be more economic, and have less customer impact than capping additional network capacity build and solving all congestion in operational timescales. However, well established economic principles such as cost reflectivity must apply.

Drafting Issues

We note that an obligation is being placed upon the DCC to annually review each Monthly Service Metric and associated Monthly Service Threshold, and to report on such to the SEC Panel (SEC H3.41). The SEC Panel should be required to give their consent to any changes that the DCC are proposing within this review, however this "SEC Panel Consent" process is not captured within the proposed legal drafting of the SEC.

Security Requirements:
Q17 Do you have any comments on the security obligations set out in Section G of the SEC drafting or the way they are expressed?

We support the proposed text, but with some concerns and items for clarification.

On the whole we are generally comfortable with the drafting that has been proposed within SEC Section G, however there are a number of areas where we believe further clarity is required, as detailed within our comments below:

Staff related obligations in G4.1 and G4.2. Whilst we recognise the need for properly qualified staff, the full requirements of BS7858:2012 need working through in terms of timing and cost impact

General Comments
There is a lack of detail regarding "Timeliness" of carrying out activities within Section G as a whole which we believe should be addressed. For example, how long should the audit logs referenced within G2.6a be retained? How long would we get to migrate to a new version of the ICO Standards referenced within G5.12?

We note from the SEC Section G workshop that was held on the 11th November, that DECC's intention is that the term "User Systems" should cover Head End Systems not back office systems therefore customer management systems, billing systems and any systems that use information retrieved from Devices should fall out of scope of the definition. This does not come across within the proposed legal drafting however, and we therefore request that the definition of "User Systems" is reviewed and updated to reflect the intent.

The definition of Type 1 and Type 2 used within this SEC document does not reflect the current definitions being used at industry working groups, for example the CPA Group. Clarity regarding these definitions is required as soon as possible.

Specific Comments:

Section G2 is entitled "SYSTEM SECURITY: OBLIGATION ON THE DCC, Unauthorised Activities: Duties to Detect and Respond" however the drafting makes no reference to Response activities at all, which we believe should be addressed;

G2.9b – As was stated at the recent SEC2 Section G (Security) Page Turning workshop, there was noted the risk that it may not be possible for the DCC to meet this absolute obligation

G2.10 – We believe the drafting here should make reference to Section G2.1 to G2.9 (not just Sections G2.1 to G2.7 as currently drafted);

G2.10 – The Term "DCC Information Security Management System" is not included in the Glossary;

G2.12 – We note that this obligation will only apply from the point at which the SEC2 drafting comes into effect. It would seem sensible for the spirit of this to operate in the intervening period, especially given that a lot of design and development work on the end to end solution will have been undertaken prior to the SEC2 Effective From Date .

G2.15(b) – Would it be more appropriate for this notification to go to the SEC Panel (who could cascade down to their Security Sub-Committee) rather than directly to the Security Sub-Committee)?

G2.22 – For the purposes of future proofing the SEC suggest that the following text is inserted after G2.22b

> "(c) any equivalent to that CESG Good Practice Guide which updates or replaces it from time to time";

G2.24 should be augmented to also include:

> " (f) patterns of traffic over the SM User WAN"

In order to capture any attempts that may be made to try and compromise the DCC via the SM User WAN;

G3.3a - We believe that usage of the term "all" within Clause 3.3a is overly onerous, and propose that the drafting is amended to reference "in line with good industry practice" rather than the term "all";

G3.7 – G3.9 - This section makes no reference to Registration Data Providers' requirements to Manage Vulnerabilities, and neither is this requirement picked up in section E2.14. We believe that the RDPs should have obligations regarding the Management of Vulnerabilities and therefore ask that consideration is given to some appropriate redrafting;

G3.12 – G3.13 – These obligations should be upon both Supplier Parties and Network Parties (not just Supplier Party as currently drafted). Note that at the SEC Section G Workshop that was held on the 11th November it was agreed that G3.13b drafting should be "on the detection of" rather than "on the occurrence of";

G4: The RDPs should also have obligations regarding organisational security. We therefore suggests that this section of the SEC is redrafted accordingly;

G4.5 – We note that at the SEC Section G Workshop that was held on the 11th November that DECC advised that they would be sponsoring the Security Check clearances referred to within this clause;

G4.6b – the definition of Privileged Person needs to be tightened;

G5.11d – suggest replace "serious incidents" with one of the relevant defined terms, for example Major Security Incident or Major Incident; and

G5.10, G5.11, G5.19 - These clauses all reference Incident Management, however they make no reference to SEC Section H (Incident Management). Insertion of a cross reference would be useful.

Security Requirements:
Q18 Do you have any comments on the appropriateness and / or the proportionality of the security obligations in relation to particular types of DCC Service Users and their role?

We are generally supportive of the security obligations, as drafted, but have some additional comments for further consideration.

We have the following general comments that we would like to make with regard to section G of the SEC as it is currently drafted:

- We have concerns around the lack of obligations being placed upon RDPs and believed that the Code should be strengthened in this area to ensure that appropriate, balanced and reciprocal arrangements are in place for all User categories. We believe that this weakness need to be addressed as soon as possible given the importance of Registration Data to the industry processes;
- We welcome and support the baseline level of control requirements that have now been captured in the drafting; and
- We are pleased to see that in general terms all Supplier Parties are being treated equally.