SECTION G - SECURITY

G7 SECURITY SUB-COMMITTEE

Establishment of the Security Sub-Committee

G7.1 The Panel shall establish a Sub-Committee in accordance with the requirements of this Section G7, to be known as the "**Security Sub-Committee**".

G7.2 Save as expressly set out in this Section G7, the Security Sub-Committee shall be subject to the provisions concerning Sub-Committees set out in Section C6 (Sub-Committees).

Membership of the Security Sub-Committee

G7.3 The Security Sub-Committee shall be composed of the following persons (each a "**Security Sub-Committee Member**"):

(a) the Security Sub-Committee Chair (as further described in Section G7.5);

(b) eight Security Sub-Committee (Supplier) Members (as further described in Section G7.6);

(c) two Security Sub-Committee (Network) Members (as further described in Section G7.8);

(d) one Security Sub-Committee (Other User) Member (as further described in Section G7.10);

(e) one Security Sub-Committee (Shared Resource Provider) Member (as further described in Section G7.12);

(f) one representative of the DCC (as further described in Section G7.15).

G7.4 Each Security Sub-Committee Member must be an individual (and cannot be a body corporate, association or partnership). No one person can hold more than one office as a Security Sub-Committee Member at the same time.

G7.5 The "**Security Sub-Committee Chair**" shall be such person as is (from time to time) appointed to that role by the Panel in accordance with a process designed to ensure that:

(a) the candidate selected is sufficiently independent of any particular Party or class of Parties;

(b) the Security Sub-Committee Chair is appointed for a [three-year] term (following which he or she can apply to be re-appointed);

(c) the Security Sub-Committee Chair is remunerated at a reasonable rate;

(d) the Security Sub-Committee Chair's appointment is subject to Section C6.9 (Member Confirmation), and to terms equivalent to Section C4.6 (Removal of Elected Members); and

(e) provision is made for the Security Sub-Committee Chair to continue in office for a reasonable period following the end of his or her term of office in the event of any delay in appointing his or her successor.

G7.6 Each of the eight "**Security Sub-Committee (Supplier) Members**" shall (subject to any directions to the contrary made by the Secretary of State for the purpose of transition on the incorporation of this Section G7 into this Code):

(a) be appointed in accordance with Section G7.7, subject to compliance by the appointed person with Section C6.9 (Member Confirmation);

(b) retire two years after his or her appointment (without prejudice to his or her ability to be nominated for a further term of office); and

(c) be capable of being removed from office in accordance with Sections C4.5 and C4.6 (Removal of Elected Members), for which purpose those Sections shall be read as if references to "Elected Member" were to "Security Sub-Committee (Supplier) Member", references to "Panel" were to "Security Sub-Committee", references to "Panel Chair" were to "Security Sub-Committee Chair", and references to "Panel Members" were to "Security Sub-Committee Members".

G7.7 Each of the eight Security Sub-Committee (Supplier) Members shall (subject to Section G7.14) be appointed in accordance with a process:

(a) by which six Security Sub-Committee (Supplier) Members will be elected by

Large Supplier Parties, and two Security Sub-Committee (Supplier) Members will be elected by Small Supplier Parties; and

(b) that is otherwise the same as that by which Elected Members are elected under Sections C4.2 and C4.3 (as if references therein to "Panel" were to "Security Sub-Committee", references to "Panel Chair" were to "Security Sub-Committee Chair", references to "Panel Members" were to "Security Sub-Committee Members", and references to provisions of Section C or D were to the corresponding provisions set out in or applied pursuant to this Section G7).

G7.8 Each of the two "**Security Sub-Committee (Network) Members**" shall (subject to any directions to the contrary made by the Secretary of State for the purpose of transition on the incorporation of this Section G7 into this Code):

(a) be appointed in accordance with Section G7.9, subject to compliance by the appointed person with Section C6.9 (Member Confirmation);

(b) retire two years after his or her appointment (without prejudice to his or her ability to be nominated for a further term of office); and

(c) be capable of being removed from office in accordance with Sections C4.5 and C4.6 (Removal of Elected Members), for which purpose those Sections shall be read as if references to "Elected Member" were to "Security Sub-Committee (Network) Member", references to "Panel" were to "Security Sub-Committee", references to "Panel Chair" were to "Security Sub-Committee Chair", and references to "Panel Members" were to "Security Sub-Committee Members".

G7.9 Each of the two Security Sub-Committee (Network) Members shall (subject to Section G7.14) be appointed in accordance with a process:

(a) by which one Security Sub-Committee (Network) Member will be elected by the Electricity Network Parties and one Security Sub-Committee (Network) Member will be elected by the Gas Network Parties; and

(b) that is otherwise the same as that by which Elected Members are elected under

Sections C4.2 and C4.3 (as if references therein to "Panel" were to "Security Sub-Committee", references to "Panel Chair" were to "Security Sub-Committee Chair", references to "Panel Members" were to "Security Sub-Committee Members", and references to provisions of Section C or D were to the corresponding provisions set out in or applied pursuant to this Section G7).

G7.10 The "**Security Sub-Committee (Other User) Member**" shall (subject to any directions to the contrary made by the Secretary of State for the purpose of transition on the incorporation of this Section G7 into this Code):

(a) be appointed in accordance with Section G7.11, subject to compliance by the appointed person with Section C6.9 (Member Confirmation);

(b) retire two years after his or her appointment (without prejudice to his or her ability to be nominated for a further term of office); and

(c) be capable of being removed from office in accordance with Sections C4.5 and C4.6 (Removal of Elected Members), for which purpose those Sections shall be read as if references to "Elected Member" were to "Security Sub-Committee (Other User) Member", references to "Panel" were to "Security Sub-Committee", references to "Panel Chair" were to "Security Sub-Committee Chair", and references to "Panel Members" were to "Security Sub-Committee Members".

G7.11 The Security Sub-Committee (Other User) Member shall (subject to Section G7.14) be appointed in accordance with a process:

(a) by which he or she is elected by those Other SEC Parties which are Other Users; and

(b) that is otherwise the same as that by which Elected Members are elected under Sections C4.2 and C4.3 (as if references therein to "Panel" were to "Security Sub-Committee", references to "Panel Chair" were to "Security Sub-Committee Chair", references to "Panel Members" were to "Security Sub-Committee Members", and references to provisions of Section C or D were to the corresponding provisions set out in or applied pursuant to this Section G7).

G7.12 The "**Security Sub-Committee (Shared Resource Provider) Member**" shall:

(a) be appointed in accordance with Section G7.13, subject to compliance by the appointed person with Section C6.9 (Member Confirmation);

(b) retire two years after his or her appointment (without prejudice to his or her ability to be nominated for a further term of office); and

(c) be capable of being removed from office in accordance with Sections C4.5 and C4.6 (Removal of Elected Members), for which purpose those Sections shall be read as if references to “Elected Member” were to “Security Sub-Committee (Shared Resource Provider) Member”, references to “Panel” were to “Security Sub-Committee”, references to “Panel Chair” were to “Security Sub-Committee Chair”, and references to “Panel Members” were to “Security Sub-Committee Members”.

G7.13 The Security Sub-Committee (Shared Resource Provider) Member shall (subject to Section G7.14) be appointed in accordance with a process:

(a) by which he or she is elected by those Other SEC Parties which are Shared Resource Providers; and

(b) that is otherwise the same as that by which Elected Members are elected under Sections C4.2 and C4.3 (as if references therein to “Panel” were to “Security Sub-Committee”, references to “Panel Chair” were to “Security Sub-Committee Chair", references to “Panel Members” were to “Security Sub-Committee Members”, and references to provisions of Section C or D were to the corresponding provisions set out in or applied pursuant to this Section G7).

G7.14 The following shall apply in respect of all candidates nominated or re-nominated for election as a Security Sub-Committee (Supplier) Member, Security Sub-Committee (Network) Member, Security Sub-Committee (Other User) Member or Security Sub-Committee (Shared Resource Provider) Member:

(a) the Security Sub-Committee may, by no later than 5 Working Days following the expiry of the period of time set out in the request for nominations, reject a candidate (by notifying the candidate of such rejection) where the Security Sub-Committee determines that the candidate does not satisfy one or more of the following requirements:

(i) the candidate must have been nominated by a company or other organisation, and the individual who submitted the nomination on behalf of the organisation must hold a senior position within the organisation;

(ii) the organisation which nominated the candidate must have confirmed that it is satisfied that the candidate has the relevant security expertise in relation to the category of membership of the Security Sub-Committee for which the candidate has been nominated;

(iii) the organisation which nominated the candidate must have confirmed that the candidate has successfully completed a BS7858 security assessment (or a security assessment named by such organisation which the organisation confirms to be equivalent); and

(iv) the candidate must have sufficient security expertise in relation to the category of membership of the Security Sub-Committee for which the candidate has been nominated;

(b) a candidate who is rejected under paragraph (a) above shall not (subject to paragraph (c) below) be an eligible candidate for the relevant election;

(c) where a candidate disputes a rejection notification under paragraph (a) above, the candidate shall have 3 Working Days following receipt of such notification to refer the matter to the Panel for its final determination of whether the candidate satisfies the requirements set out in paragraph (a) above; and

(d) where necessary, the Secretariat shall delay giving notice of the names of eligible candidates pending expiry of the time periods set out in paragraph (a) and/or (c) or determination by the Panel under paragraph (c) (as applicable).

G7.15 The DCC may nominate one person to be a Security Sub-Committee Member by notice to the Secretariat from time to time. The DCC may replace its nominee from time to time by prior notice to the Secretariat. Such nomination or replacement shall be subject to compliance by the relevant person with Section C6.9 (Member Confirmation).

Proceedings of the Security-Sub Committee

G7.16 Without prejudice to the generality of Section C5.13(c) (Attendance by Other Persons) as it applies pursuant to Section G7.17:

(a) a representative of the Secretary of State and a representative of the Authority shall be:

(i) invited to attend each and every Security Sub-Committee meeting;

(ii) entitled to speak at such Security Sub-Committee meetings without the permission of the Security Sub-Committee Chair; and

(iii) provided with copies of all the agenda and supporting papers available to Security Sub-Committee Members in respect of such meetings;

(b) the Security Sub-Committee Chair shall invite to attend Security Sub-Committee meetings any persons that the Security Sub-Committee determines it appropriate to invite in order to be provided with expert advice on security matters.

G7.17 Subject to Section G7.16, the provisions of Section C5 (Proceedings of the Panel) shall apply to the proceedings of the Security Sub-Committee, for which purpose that Section shall be read as if references to “Panel” were to “Security Sub-Committee”, references to “Panel Chair” were to “Security Sub-Committee Chair”, and references to “Panel Members” were to “Security Sub-Committee Members”.

Duties and Powers of the Security Sub-Committee

G7.18 The Security Sub-Committee:

(a) shall perform the duties and may exercise the powers set out in Sections G7.19

to G7.23; and

(b) shall perform such other duties and may exercise such other powers as may be expressly ascribed to the Security Sub-Committee elsewhere in this Code.

Document Development and Maintenance

G7.19 The Security Sub-Committee shall:

(a) develop and maintain a document, to be known as the "**Security Controls Framework**", which shall:

(i) set out the appropriate User Security Assessment Methodology to be applied to different categories of security assurance assessment carried out in accordance with Section G8 (User Security Assurance); and

(ii) be designed to ensure that such security assurance assessments are proportionate, consistent in their treatment of equivalent Users and equivalent User Roles, and achieve appropriate levels of security assurance in respect of different Users and different User Roles;

(b) carry out reviews of the Security Risk Assessment:

(i) at least once each year in order to identify any new or changed security risks to the End-to-End Smart Metering System; and

(ii) in any event promptly if the Security Sub-Committee considers there to be any material change in the level of security risk;

(c) maintain the Security Requirements to ensure that it is up to date and at all times identifies the security controls which the Security Sub-Committee considers appropriate to mitigate the security risks identified in the Security Risk Assessment;

(d) maintain the End-to-End Security Architecture to ensure that it is up to date;

(e) develop and maintain a document to be known as the "**Risk Treatment Plan**", which shall identify the residual security risks which in the opinion of the Security Sub-Committee remain unmitigated taking into account the security controls that are in place; and

(f) liaise and work with the NCSC to develop and maintain CPA Security Characteristics that set out the levels of security required for Smart Meters, Communications Hubs, SAPCs and HCALCs that are proportionate and appropriate taking into consideration the security risks identified in the Security Risk Assessment.

Security Assurance

G7.20 The Security Sub-Committee shall:

(a) periodically, and in any event at least once each year, review the Security Obligations and Assurance Arrangements in order to identify whether in the opinion of the Security Sub-Committee they continue to be fit for purpose;

(b) exercise such functions as are allocated to it under, and comply with the applicable requirements of Section G8 (User Security Assurance) and Section G9 (DCC Security Assurance);

(c) provide the Panel with support and advice in respect of issues relating to the actual or potential non-compliance of any Party with the requirements of the Security Obligations and Assurance Arrangements;

(d) keep under review the NCSC CPA Certificate scheme in order to assess whether it continues to be fit for purpose in so far as it is relevant to the Code, and suggest modifications to the scheme provider to the extent to which it considers them appropriate;

(e) to the extent to which it considers it appropriate, in relation to any User (or, during the first User Entry Process, Party) which has produced a User Security Assessment Response that sets out any steps that the User proposes to take in accordance with Section G8.24(b):

(i) liaise with that User (or Party) as to the nature and timetable of such steps;

(ii) either accept the proposal to take those steps within that timetable or seek to agree with that User (or Party) such alternative steps or timetable as the Security Sub-Committee may consider appropriate; and

(iii) take advice from the User Independent Security Assurance Service Provider; and

(iv) where the Security Sub-Committee considers it appropriate, request the User Independent Security Assurance Service Provider to carry out a Follow-up Security Assessment;

(f) provide advice to the Panel on the scope and output of the independent security assurance arrangements of the DCC in relation to the design, building and testing of the DCC Total System;

(g) provide advice to the Panel on the scope and output of the SOC2 assessment of the DCC Total System;

(h) provide advice to the Panel in relation to the appointment of the User Independent Security Assurance Service Provider, monitor the performance of the person appointed to that role and provide advice to the Panel in respect of its views as to that performance; and

(i) provide advice and information to the Authority in relation to any actual or potential non-compliance with the CPA Security Characteristics of any Device or apparatus in respect of which a CPA Certificate is issued or required.

Monitoring and Advice

G7.21 The Security Sub-Committee shall:

(a) provide such reasonable assistance to the DCC and Users as may be requested by them in relation to the causes of security incidents and the management of vulnerabilities on their Systems;

(b) monitor the (actual and proposed) Anomaly Detection Thresholds of which it is notified by the DCC, consider the extent to which they act as an effective means of detecting any Compromise to any relevant part of the DCC Total System or of any User Systems, and provide its opinion on such matters to the

DCC;

(c) provide the Panel with support and advice in respect of Disputes for which the Panel is required to make a determination, insofar as such Disputes relate to the Security Obligations and Assurance Arrangements;

(d) provide the Panel, the Change Sub-Committee, the Change Board and any relevant Working Group with support and advice in relation to any Draft Proposal or Modification Proposal which may affect the security of the End-to-End Smart Metering System or the effective implementation of the security controls that are identified in the Security Requirements;

(e) advise the Authority of any modifications to the conditions of Energy Licences which it considers may be appropriate having regard to the residual security risks identified from time to time in the Risk Treatment Plan;

(f) respond to any consultations on matters which may affect the security of the End-to-End Smart Metering System or the effective implementation of the security controls that are identified in the Security Requirements;

(g) act in cooperation with, and send a representative to, the SMKI PMA, the Technical Architecture and Business Architecture Sub-Committee and any other Sub-Committee or Working Group which requests the support or attendance of the Security Sub-Committee;

(h) (to the extent to which it reasonably considers that it is necessary to do so) liaise and exchange information with, provide advice to, and seek the advice of the At HAN Forum on matters relating to the Alt HAN Arrangements which may affect the security of the End-to-End Smart Metering System or the effective implementation of the security controls that are identified in the Security Requirements;

(i) provide such further support and advice to the Panel as it may request; and

(j) provide the Authority with such information and documents as it may reasonably request in relation to any matter referred by a Party to the Authority for determination pursuant to Section F2.7B.

Modifications

G7.22 The Security Sub-Committee shall establish a process under which the Code Administrator monitors Draft Proposals and Modification Proposals with a view to identifying (and bringing to the attention of the Security Sub-Committee) those proposals that:

(a) are likely to affect the Security Obligations and Assurance Arrangements; or

(b) are likely to relate to other parts of the Code but may have a material effect on the security of the End-to-End Smart Metering System,

and the Code Administrator shall comply with such process.

G7.23 Notwithstanding Section D1.3 (Persons Entitled to Submit Draft Proposals):

(a) the Security Sub-Committee shall be entitled to submit Draft Proposals in respect of the Security Obligations and Assurance Arrangements where the Security Sub-Committee considers it appropriate to do so; and

(b) any Security Sub-Committee Member shall be entitled to submit Draft Proposals in respect of the Security Obligations and Assurance Arrangements where he or she considers it appropriate to do so (where the Security Sub-Committee has voted not to do so).

G7.24 Notwithstanding and subject to the provisions of the Working Group Terms of Reference, the Security Sub-Committee shall be entitled to nominate a representative to be a member of any Working Group.

G7.25 For the purposes of Section D7.1 (Modification Report):

(a) written representations in relation to the purpose and effect of a Modification Proposal may be made by:

(i) the Security Sub-Committee; and/or

(ii) any Security Sub-Committee Member (either alone or in addition to any representations made by other Security Sub-Committee Members and/or the Security Sub-Committee collectively); and

(b) notwithstanding Section D7.3 (Content of the Modification Report), the Code Administrator shall ensure that all such representations, and a summary of any evidence provided in support of them, are set out in the Modification Report prepared in respect of the relevant Modification Proposal.