

## **SECTION G - SECURITY**

### **G3 SYSTEM SECURITY: OBLIGATIONS ON USERS**

#### **Unauthorised Activities: Duties to Detect and Respond**

G3.1 Each User shall:

- (a) take reasonable steps to ensure that:
  - (i) its User Systems are capable of identifying any deviation from their expected configuration; and
  - (ii) any such identified deviation is rectified; and
- (b) for these purposes maintain at all times an up-to-date list of all hardware, and of all software and firmware versions and patches, which form part of the configuration of those User Systems.

G3.2 Each User shall take reasonable steps:

- (a) to ensure that its User Systems are capable of detecting any unauthorised software that has been installed or executed on them and any unauthorised attempt to install or execute software on them;
- (b) if those User Systems detect any such software or such attempt to install or execute software, to ensure that the installation or execution of that software is prevented; and
- (c) where any such software has been installed or executed, to take appropriate remedial action.

G3.3 Each User shall:

- (a) ensure that its User Systems record all attempts to access resources, or Data held, on them;
- (b) ensure that its User Systems detect any attempt by any person to access resources, or Data held, on them without possessing the authorisation required

to do so; and

- (c) take reasonable steps to ensure that its User Systems prevent any such attempt at unauthorised access.

### **Security Incident Management**

G3.4 Each User shall ensure that, on the detection of any unauthorised event of the type referred to at Sections G3.1 to G3.3, it takes all of the steps required by its User Information Security Management System.

G3.5 Each User shall, on the occurrence of a Major Security Incident in relation to its User Systems, ensure that the Panel and the Security Sub-Committee are promptly notified.

### **System Design and Operation**

G3.6 Each User shall, at each stage of the System Development Lifecycle, have regard to the need to design and operate its User Systems so as to protect them from being Compromised.

### **Management of Vulnerabilities**

G3.7 Each Supplier Party shall ensure that either a tester who has achieved CREST certification or an organisation which is a CHECK service provider carries out assessments that are designed to identify any vulnerability of its User Systems to Compromise:

- (a) in respect of each of its User Systems, on at least an annual basis;
- (b) in respect of each new or materially changed component or functionality of its User Systems, prior to that component or functionality becoming operational; and
- (c) on the occurrence of any Major Security Incident in relation to its User Systems.

G3.8 Each User shall ensure that it carries out assessments that are designed to identify any vulnerability of its User Systems to Compromise:

- (a) in respect of each of its User Systems, on at least an annual basis;

- (b) in respect of each new or materially changed component or functionality of its User Systems, prior to that component or functionality becoming operational; and

on the occurrence of any Major Security Incident in relation to its User Systems.

G3.9 Each User shall ensure that:

- (a) in respect of any new or materially changed component or functionality of its User Systems which comprises (or includes) a System that is being incorporated into its User Systems for the first time:
  - (i) it notifies the Security Sub-Committee prior to that System becoming an operational part of its User Systems;
  - (ii) together with that notification it provides to the Security Sub-Committee an adequate description of the System, of the purpose for which it will be used, and of the nature of its relationship to the other component parts of the User Systems; and
  - (iii) that System does not become an operational part of its User Systems unless and until the Security Sub-Committee has authorised the User to bring it into operation (for which purpose, following any such review or assessment as it may consider appropriate, the Security Sub-Committee shall be entitled to give or withhold authorisation by means of notice to the User); and
- (b) where, following any assessment of its User Systems in accordance with Section G3.7 or G3.8, any material vulnerability has been detected, a User shall ensure that it:
  - (i) takes reasonable steps to ensure that the cause of the vulnerability is rectified, or the potential impact of the vulnerability is mitigated, as soon as is reasonably practicable;
  - (ii) promptly notifies the Security Sub-Committee of the steps being taken to rectify its cause or mitigate its potential impact (as the case may be) and the time within which they are intended to be completed; and

- (c) where a material component or material functionality of its User Systems is being discontinued or where a User System is being decommissioned;
  - (i) the User notifies the Security Sub-Committee prior to the component or functionality being discontinued or the User System being decommissioned (as relevant);
  - (ii) together with that notification, the User provides to the Security Sub-Committee an adequate description of the reason for the change and the proposed timing of the change;
  - (iii) the discontinuation or decommissioning is not undertaken before the Security Sub-Committee has been notified; and
  - (iv) the User takes any reasonable action advised by the Security Sub-Committee.

### **Management of Data**

G3.10 Each User shall:

- (a) develop and maintain, and hold all Data in accordance with, a User Data Retention Policy; and
- (b) when any Data held by it cease to be retained in accordance with the User Data Retention Policy, ensure that they are securely deleted in accordance with its Information Classification Scheme.

### **User Systems: Duty to Separate**

G3.11 Each User shall take reasonable steps to ensure that any software or firmware that is installed on its User Systems for the purposes of security is Separated from any software or firmware that is installed on those Systems for any other purpose.

### **User Systems: Independence of DCC Live Systems**

G3.12 Each User shall ensure that no individual is engaged in:

- (a) the development of bespoke software or firmware, or the customisation of any software or firmware, for the purpose of its installation on any part of its User

Systems; or

- (b) the development, design, build, testing, configuration, implementation, operation, maintenance, modification or decommissioning of any part of its User Systems,

unless that individual satisfies the requirements of Section G3.13.

G3.13 An individual satisfies the requirements of this Section only if, at any time at which that individual is engaged in any activity described in Section G3.12, he or she:

- (a) is not at the same time also engaged in:
  - (i) the development of bespoke software or firmware, or the customisation of any software or firmware, for the purpose of its installation on any part of the DCC Live Systems; or
  - (ii) the development, design, build, testing, configuration, implementation, operation, maintenance, modification or decommissioning of any part of the DCC Live Systems; and
- (b) has not been engaged in any activity described in paragraph (a) for a period of time which the User reasonably considers to be appropriate, having regard to the need to ensure the management of risk in accordance with its User Information Security Management System.

G3.14 Each User shall ensure that no resources which form part of its User Systems also form part of the DCC Live Systems.

### **Monitoring**

G3.15 Each Supplier Party shall take reasonable steps to ensure that its User Systems are capable of detecting Anomalous Events, in particular by reference to the:

- (a) sending or receipt (as the case may be) of Service Requests, Pre-Commands, Signed Pre-Commands, Service Responses and Alerts;
- (b) audit logs of each Device for which it is the Responsible Supplier; and
- (c) error messages generated by each Device for which it is the Responsible

Supplier.

G3.16 Each Supplier Party shall:

- (a) take reasonable steps to ensure that its User Systems detect all Anomalous Events; and
- (b) ensure that, on the detection by its User Systems of any Anomalous Event, it takes all of the steps required by its User Information Security Management System.

**Manufacturers: Duty to Notify and Be Notified**

G3.17 Where a User becomes aware of any material security vulnerability in, or likely cause of a material adverse effect on the security of:

- (a) any hardware, software or firmware which forms part of its User Systems; or
- (b) (where applicable) any Smart Metering System (excluding a Communications Hub Function or Gas Proxy Function which forms part of a SMETS2+ Device) for which it is the Responsible Supplier,

it shall comply with the requirements of Section G3.18.

G3.18 The requirements of this Section are that the User shall:

- (a) wherever it is reasonably practicable to do so notify the manufacturer of the hardware or Device or the developer of the software or firmware (as the case may be);
- (b) take reasonable steps to ensure that the cause of the vulnerability or likely cause of the material adverse effect is rectified, or its potential impact is mitigated, as soon as is reasonably practicable; and
- (c) ensure that the Security Sub-Committee is promptly notified of the steps being taken to rectify the cause of the vulnerability or likely cause of the material adverse effect, or to mitigate its potential impact (as the case may be), and the time within which those steps are intended to be completed.

G3.19 A User shall not be required to notify a manufacturer or developer in accordance with

Section G3.18(a) where it has reason to be satisfied that the manufacturer or developer is already aware of the matter that would otherwise be notified.

G3.20 Each User shall, wherever it is practicable to do so, establish with:

- (a) the manufacturers of the hardware and developers of the software and firmware which form part of its User Systems; and
- (b) (where applicable) any Smart Metering System (excluding a Communications Hub Function or Gas Proxy Function which forms part of a SMETS2+ Device) for which it is the Responsible Supplier,

arrangements designed to ensure that the User will be notified where any such manufacturer or developer (as the case may be) becomes aware of any material security vulnerability in, or likely cause of a material adverse effect on the security of, such hardware, software, firmware or Device.

G3.21 Any arrangements established in accordance with Section G3.20 may provide that the manufacturer or developer (as the case may be) need not be required to notify the User where that manufacturer or developer has reason to be satisfied that the User is already aware of the matter that would otherwise be notified under the arrangements.

[G3.21A Where a CPL Manufacturer becomes aware of any material security vulnerability in, or likely cause of a material adverse effect on, the security of any Device Model in respect of which it is the CPL Manufacturer, it shall comply with the requirements of Section G3.18\(b\) and \(c\).](#)

### **Cryptographic Processing**

G3.22 Each User shall ensure that it carries out Cryptographic Processing only within Cryptographic Modules established in accordance with its Information Classification Scheme.

### **User Systems: Physical Location**

G3.23 Each User which is an Eligible User in relation to any Supply Sensitive Service Request shall ensure that:

- (a) any Cryptographic Module which constitutes a component of its User Systems

and in which:

- (i) any Private Key that is used to Digitally Sign Pre-Commands is held;
  - (ii) Pre-Commands are Digitally Signed; and
  - (iii) any SMETS1 Service Request that constitutes a Critical Service Request is Digitally Signed; and
- (b) any functionality of its User Systems which is used to apply Supply Sensitive Checks,

is located, operated, configured, tested and maintained in the United Kingdom by User Personnel who are located in the United Kingdom.

G3.24 Each User to which Section G3.23 applies shall ensure that the components and the functionality of its User Systems to which that Section refers are operated from a sufficiently secure environment in accordance with the provisions of Section G5.17.

#### **Supply Sensitive Check**

G3.25 Each User which is an Eligible User in relation to any Supply Sensitive Service Request shall ensure that:

- (a) it applies a Supply Sensitive Check prior to Digitally Signing a Pre-Command or SMETS1 Service Request in respect of any Supply Sensitive Service Request;
- (b) it both applies that Supply Sensitive Check and Digitally Signs the relevant Pre-Command or SMETS1 Service Request in the United Kingdom; and
- (c) the relevant Pre-Command or SMETS1 Service Request has been processed only in the United Kingdom between the application of the Supply Sensitive Check and the Digital Signature.

#### **SMETS1 Smart Metering Systems**

G3.26 Each Supplier Party shall use its best endeavours to ensure that each SMETS1 SMS for which it is the Responsible Supplier is at all times Secure.

G3.27 Each Supplier Party shall retain documentary evidence sufficient to demonstrate its compliance with the obligation at Section G3.26.

G3.28 For the purposes of Section G3.26:

- (a) a SMETS1 SMS is "**Secure**" if it is designed, installed, operated and supported so as to ensure, to an Appropriate Standard, that it is not subject to any event which results, or is capable of resulting, in any Device of which it is comprised being Compromised to a material extent; and
- (b) an "**Appropriate Standard**" means a high level of security that is in accordance with good industry practice within the energy industry in Great Britain, and is capable of verification as such by the User Independent Security Assurance Service Provider in accordance with Section G8.

**User Use of Private Keys**

G3.29 Each User shall ensure that any Private Key that it uses or intends to use to create a Digital Signature that forms part of a Command that is to be sent to a SMETS2+ Device is used only for the purposes of:

- (a) creating Digital Signatures that form part of Commands that are to be sent to SMETS2+ Devices; or
- (b) Digitally Signing Certificate Signing Requests.

**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 Security Sub-Committee (CPL Manufacturer) Member as further described in Section G7.13A; and
  - ~~(g)~~ (g) 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);
- (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; and
- (f) where the Security Sub-Committee Chair's appointment (and for the purposes of this Section and Section G7.5A all references to appointment shall encompass re-appointment) is to take effect on or after the date this Section G7.5(f) comes into force, the Panel shall:
  - (i) notify the Secretary of State of the appointment it proposes to make;
  - (ii) not make the appointment unless and until the Secretary of State has confirmed in writing that they do not object to the appointment being made;
  - (iii) ensure that the terms of the appointment include terms which provide for the Panel to terminate the appointment where directed to do so by the Secretary of State pursuant to Section G7.5A and from such date or within such period as may be specified in the Secretary of State's direction; and
  - (iv) where the appointed person has not, at the date of the appointment, passed (as a minimum) a Security Check (or equivalent), ensure that the

terms of the appointment include terms which:

- (A) require the appointed person to apply for a Security Check (or equivalent) within one month of the date of the appointment;
- (B) provide for the Panel to terminate the appointment if a Security Check (or equivalent) is not passed by the appointed person within 12 months of the date of the appointment (or such longer period as the Secretary of State may approve following a request from the Panel).

G7.5A The Secretary of State may, in respect of any Security Sub-Committee Chair appointment which takes effect on or after the date Section G7.5(f) comes into force, direct the Panel to terminate the appointment of the Security Sub-Committee Chair where the Secretary of State considers it necessary to do for the purposes of preserving the integrity of, and in the interests of maintaining, the security of the End-to-End Smart Metering System (or any part of that system).

G7.5B The Panel shall comply with any direction given to it by the Secretary of State pursuant to Section G7.5A.

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).

G7.13A The "**Security Sub-Committee (CPL Manufacturer) Member**" shall:

- (a) be appointed in accordance with Section G7.13B, 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 (CPL Manufacturer) 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”.

G7.13B The Security Sub-Committee (CPL Manufacturer) 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 CPL Manufacturers; 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 or Security Sub-Committee (CPL Manufacturer) 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 documents, to be known as the "**Security Controls Framework**", which shall set out the appropriate User and DCC Security Assessment Methodology to be applied to different categories of security assurance assessment carried out in accordance with Section G8 (User Security Assurance) and Section G9 (DCC Security Assurance) and be designed to ensure that such security assurance assessments are proportionate; and
  - (i) achieve appropriate levels of security assurance in respect of different Users and different User Roles, and the DCC; and
  - (ii) in the case of User related assessments are consistent in their treatment of equivalent Users and equivalent User Roles, and;
- (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;
- (f) with respect to the CPA Security Characteristics:
  - (i) ~~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; and

(ii) where it considers it appropriate from time to time, develop the CPA Security Characteristics so as additionally to set out levels of security required for any other Device,

in each case so as to ensure that the required levels of security are proportionate and appropriate taking into consideration the security risks identified in the Security Risk Assessment; ~~and~~

(g) develop and maintain a document to be known as the "CPA Policies and Procedures" which shall:

(i) set out the steps that a Manufacturer must follow in order to obtain and maintain a CPA Certificate in respect of a Device Model;

(ii) set out the criteria that a Test Lab must satisfy in order to perform the functions of a CPA Test Lab for the purposes of the CPA Scheme;

(iii) describe the procedures that a CPA Test Lab must apply in evaluating whether a Device Model should be issued with a CPA Certificate;

(iv) make such other provision in relation to the evaluation and assessment of a Device Model for the purposes of the CPA Scheme as the Security Sub-Committee may consider appropriate;

(v) make such other provision in relation to the obligations of Manufacturers and CPA Test Labs for the purposes of the CPA Scheme as the Security Sub-Committee may consider appropriate;

(vi) make such provision relating to the expiry, renewal, suspension, withdrawal and cancellation of CPA Certificates as the Security Sub-Committee may consider appropriate; and

(vii) make such provision in relation to the role of the CPA Scheme Operator as the Security Sub-Committee may consider appropriate;

- (h) develop and maintain documents to be known as the "CPA Assurance Maintenance Plan" which shall describe the components of a Device that, if changed, will require a new CPA Certificate to be issued;
- (i) publish on the Website each CPA Certificate and all supporting documentation relating to that CPA Certificate; and
- ~~(g)~~(j) develop and maintain documents to be known as the "SSC Guidance for Device Security Assurance and Triage" which shall set out the SSC's guidance on the Security Sub-Committee in respect of the requirements and processes which are to be followed in respect of Devices (including in relation to their triage-Triage and refurbishment) in order to:
  - (i) achieve appropriate levels of security assurance in accordance with the requirement of this Code; and
  - (ii) obtain and maintain a CPA CertificationCertificate.

#### 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~~exercise such functions as are allocated to it under,

and comply with the applicable requirements of, Section G13 (CPA Scheme Operator) with the objective of ensuring that there are available at all times CPA Scheme Operator Services which are both suitable in nature and sufficient in quantity to meet the reasonable requirements of the CPA Scheme;

- (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) to the extent to which it considers appropriate , in relation to the DCC which has produced a DCC Security Assessment Response that sets out any steps that the DCC proposes to take in accordance with Section G9.24(b):
  - (i) liaise with the DCC 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 the DCC such alternative steps or timetable as the Security Sub-Committee may consider appropriate;

#### Annex 4 - Revised legal drafting – SEC Section G

- (iii) take advice from the DCC Independent Security Assessment Service Provider; and
  - (iv) where the Security Sub-Committee considers it appropriate, request the DCC Independent Security Assessment Service Provider to carry out a Follow-up Security Assessment;
- (h) provide advice to the:
- (i) 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
  - (ii) DCC in relation to the appointment of the DCC Independent Security Assessment Service Provider, monitor the performance of the person appointed to that role and provide advice to the DCC in respect of its views as to that performance;
- (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

#### Annex 4 - Revised legal drafting – SEC Section G

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.

**G9     DCC SECURITY ASSURANCE**

**The DCC Independent Security Assessment Arrangements**

G9.1 The DCC shall establish, give effect to, maintain and comply with arrangements, to be known as the "**DCC Independent Security Assessment Arrangements**", which shall procure the services of a DCC Independent Security Assessment Service Provider to undertake security assessment services.

**Scope of Security Assessment Services**

G9.2 The security assessment services specified in this Section G9.2 are services in accordance with which the DCC Independent Security Assessment Service Provider shall:

- (a) carry out DCC Security Assessments at such times and in such manner as is provided for in this Section G9;
- (b) produce DCC Security Assessment Reports in relation to the DCC that have been the subject of a DCC Security Assessment;
- (c) receive, consider and validate DCC Security Assessment Responses and carry out any Follow-up Security Assessments at the request of the Security Sub-Committee;
- (d) otherwise, at the request of, and to an extent determined by, the Security Sub-Committee, carry out an assessment of the compliance of the DCC with its obligations under:
  - (i) Condition 8 (Security Controls for the Authorised Business) of the DCC Licence;
  - (ii) the requirements of Sections G2 and G4 to G6 or any CPA Certificate Remedial Plan; and where:
  - (iii) following either a DCC Security Assessment, any material increase in the security risk relating to the DCC has been identified; or
  - (iv) the Security Sub-Committee otherwise considers it appropriate for that

assessment to be carried out;

- (e) at the request of the Security Sub-Committee, provide to it advice in relation to:
  - (i) the compliance of the DCC with its obligations under Sections G or any CPA Certificate Remedial Plan; and
  - (ii) changes in security risks relating to the Systems, Data, functionality and processes of the DCC which fall within Section G5 (Information Security: Obligations on the DCC);
- (f) at the request of the Security Sub-Committee, provide to it advice in relation to the suitability of any remedial action plan for the purposes of Section M8.4 of the Code (Consequences of an Event of Default);
- (g) at the request of the Security Sub-Committee Chair, provide a representative to attend and contribute to the discussion at any meeting of the Security Sub-Committee; and
  - (i) undertake such other activities and do so at such times and in such manner, as may be further provided for in this Section G9;
  - (ii) assess the DCC's compliance with the requirements of Condition 8 (Security Controls for the Authorised Business) of the DCC Licence;
  - (iii) such other requirements relating to the security of the DCC Total System as may be specified by the Security Sub-Committee or the Panel from time to time.

G9.3 The actions specified in this Section G9.3 shall be actions taken by the DCC to:

- (a) procure the provision of security assessment services by the DCC Independent Security Assessment Service Provider (as further described in Section G9.4);
- (b) ensure that the DCC Independent Security Assessment Service Provider carries out Security Assessments for the purpose specified in Section G9.2:
  - (i) annually;

- (ii) on any material change to the DCC Total System; and
  - (iii) at any other time specified by the Security Sub-Committee or the Panel;
- (c) comply with the arrangements set out by the Security Sub-Committee in a Security Controls Framework;
- (d) in line with the methodology and processes set out in the Security Controls Framework:
  - (i) procure that the DCC Independent Security Assessment Service Provider produces a DCC Security Assessment Report following each such assessment that has been carried out;
  - (ii) ensure that the DCC Independent Security Assessment Service Provider provides the Security Sub-Committee with a copy of each such DCC Security Assessment Report;
  - (iii) produce a DCC Security Assessment Response in relation to each such report; and
  - (iv) provide to the Panel and the Security Sub-Committee a copy of each DCC Security Assessment Response and, as soon as reasonably practicable thereafter, a report on its implementation of any action plan that is required by the Security Sub-Committee.

**The DCC Independent Security Assessment Service Provider**

G9.4 For the purposes of Section G9.3, the "**DCC Independent Security Assessment Service Provider**" shall be a person who is appointed by the DCC to provide security assessment services:

- (a) of the scope specified in Section G9.2;
- (b) from a person who:
  - (i) is suitably qualified in accordance with Section G9.5;
  - (ii) is suitably independent in accordance with Section G9.8.

**Suitably Qualified Service Provider**

G9.5 The DCC Independent Security Assessment Service Provider shall be treated as suitably qualified in accordance with this Section G9.5 only if it satisfies:

- (a) one or more of the requirements specified in Section G9.6; and
- (b) the requirement specified in Section G9.7.

G9.6 The requirements specified in this Section G9.6 are that the DCC Independent Security Assessment Service Provider:

- (a) is accredited by UKAS as meeting the requirements for providing audit and certification of information security management systems in accordance with ISO/IEC 27001:2017 Information Technology – Security Techniques – Information Security Management Systems) or any equivalent to that standard which updates or replaces it from time to time; and/or
- (b) holds another membership, accreditation, approval or form of professional validation that is in the opinion of the Security Sub-Committee substantially equivalent in status and effect to one or more of the arrangements described in paragraphs (a) and (b).

G9.7 The requirement specified in this Section G9.7 is that the DCC Independent Security Assessment Service Provider:

- (a) employs consultants who are certified under the Certified Cyber Security Consultancy (CCSC) scheme and have experience of operating at the 'Lead' or 'Senior Practitioner' level in either 'Security and Information Risk Advisor' or 'Information Assurance Auditor' roles; and
- (b) engages those individuals as its lead auditors for the purposes of carrying out all security assessments in accordance with this Section G7.

**Independence Requirement**

G9.8 The DCC Independent Security Assurance Service Provider shall be treated as suitably independent in accordance with this Section G9.8 only if it satisfies:

- (a) the requirements specified in Section G9.9; and
- (b) the requirement specified in Section G9.10.

G9.9 For the purposes of Sections G9.9 and G9.10:

- (a) the DCC must be independent from the DCC Independent Security Assessment Service Provider in carrying out functions under this Section G9; and
- (b) all of the DCC's Service Providers must be independent from the DCC Independent Security Assessment Service Provider in carrying out its functions to assess the DCC's compliance with its obligations as the DCC under Sections G2 and G4 to G6 and DCC Licence Condition 8 (Security Controls for the Authorised Business) and SEC Appendix Z Sections 6 and 7.

G9.10 The requirements specified in this Section G9.10 are that:

- (a) neither the DCC or any of its subsidiaries, and no DCC Service Provider or any of its subsidiaries, holds or acquires any investment by way of shares, securities or other financial rights or interests in the DCC Independent Security Assessment Service Provider;
- (b) no director of the DCC and no director of any DCC Service Provider, is or becomes a director or employee of, or holds or acquires any investment by way of shares, securities or other financial rights or interests in, the DCC Independent Security Assessment Service Provider; and
- (c) the DCC Independent Security Assessment Service Provider does not hold or acquire a participating interest (as defined in section 421A of the Financial Services and Markets Act 2000) in the DCC or any of the DCC's Service Providers, (for these purposes references to the DCC's Service Providers shall not include the DCC Independent Security Assessment Service Provider where it acts in that capacity).

G9.11 The requirement specified in this Section G9.11 is that the DCC Independent Security Assessment Service Provider is able to demonstrate to the satisfaction of the Security

Sub-Committee that it has in place arrangements to ensure that it will at all times act independently of any commercial relationship that it has, has had, or may in future have with the DCC or the DCC's Service Providers (and for these purpose a 'commercial relationship' shall include a relationship established by virtue of the DCC Independent Security Assessment Service Provider itself being a DCC Service Provider to the DCC).

#### **Compliance of the DCC Independent Security Assessment Service Provider**

G9.12 The Security Sub-Committee shall advise the DCC of any performance failures or non-compliance with the SEC obligations on the part of the DCC Independent Security Assessment Service Provider to enable the DCC to ensure that the DCC Independent Security Assessment Service Provider carries out its functions in accordance with the provisions of this Section ~~G12~~G9.

#### **DCC: Duty to Cooperate in Assessment**

G9.13 The DCC shall do all such things as may be reasonably requested by the Security Sub-Committee, or by any person acting on behalf of or at the request of the Security Sub-Committee (including in particular the DCC Independent Security Assessment Service Provider), for the purposes of facilitating an assessment of the DCC's compliance with its obligations under Sections G2 and G4 to G6 or DCC Licence Condition 8 (Security Controls for the Authorised Business) or SEC Appendix Z Sections 6 and 7 and any CPA Certificate Remedial Plan.

G9.14 For the purposes of Section G9.13, the DCC shall provide the DCC Independent Security Assessment Service Provider with:

- (a) all such Data as may reasonably be requested, within such times and in such format as may reasonably be specified;
- (b) all such other forms of cooperation as may reasonably be requested, including in particular:
  - (i) access at all reasonable times to such parts of the premises of the DCC or its Service Providers as are used for, and such persons engaged by the DCC as carry out or are authorised to carry out, any activities related to its compliance with its obligations under Sections G2 and G4 to G6 and

DCC Licence Condition 8 (Security Controls for the Authorised Business) and SEC Appendix Z Sections 6 and 7; and

- (ii) such cooperation as may reasonably be requested by the DCC Independent Security Assessment Services Provider for the purposes of carrying out any security assurance assessment in accordance with this Section G9.

### **Categories of DCC Security Assessment**

G9.15 For the purposes of this Section G9, there shall be the following two categories of security assessment:

- (a) a Full DCC Security Assessment (as further described in Section G9.16);
- (b) a Follow-up DCC Security Assessment (as further described in Section G9.17).

G9.16 A **“Full DCC Security Assessment”** shall be an assessment carried out by the DCC Independent Security Assessment Service Provider in respect of the DCC and its Service Providers to identify the extent to which the DCC is compliant with each of its obligations under Sections G2 and G4 to G6 and DCC Licence Condition 8 (Security Controls for the Authorised Business) and SEC Appendix Z Sections 6 and 7.

G9.17 A **“Follow-up DCC Security Assessment”** shall be an assessment carried out by the DCC Independent Security Assessment Service Provider, following a DCC Security Assessment, in accordance with the provisions of Section G9.25.

### **DCC Security Assessments: General Procedure**

#### **DCC Security Assessment Methodology**

G9.18 Each DCC Security Assessment carried out by the DCC Independent Security Assessment Service Provider shall be carried out in accordance with the Security Controls Framework developed as defined in G7.19(a).

#### **The DCC Security Assessment Report**

G9.19 Following the completion of a DCC Security Assessment, the DCC Independent

Security Assessment Service Provider shall, in discussion with the DCC, produce a written report (a "**DCC Security Assessment Report**") which shall:

- (a) set out the findings of the DCC Independent Security Assessment Service Provider on all the matters within the scope of the DCC Security Assessment;
- (b) specify any instances of actual or potential non-compliance of the DCC with its obligations under Sections G2 and G4 to G6 which have been identified by the DCC Independent Security Assessment Service Provider;
- (c) specify any instances of actual or potential non-compliance of the DCC with its obligations under DCC Licence Condition 8 (Security Controls for the Authorised Business);
- (d) specify any instances of actual or potential non-compliance of the DCC with its obligations under SEC Appendix Z, Sections 6 and 7; and
- (e) set out the evidence which, in the opinion of the DCC Independent Security Assessment Service Provider, establishes each of the instances of actual or potential non-compliance which it has identified;

G9.20 The DCC Independent Security Assessment Service Provider shall submit a copy of each DCC Security Assessment Report to the Security Sub-Committee and to the DCC.

#### The DCC Security Assessment Response

G9.21 Following the receipt by the DCC of a DCC Security Assessment Report which relates to it, the DCC shall as soon as reasonably practicable, and in any event by no later than such date as the Security Sub-Committee may specify:

- (a) produce a written response to that report (a "**DCC Security Assessment Response**") which
- (b) addresses the findings set out in the report; and
- (c) submit a copy of that response to the Security Sub-Committee and the DCC Independent Security Assessment Service Provider.

G9.22 Where a DCC Security Assessment Report following a Full DCC Security Assessment,

specifies any instance of actual or potential noncompliance of the DCC with its obligations under Sections G2 and G4 to G6 and/or with DCC Licence Condition 8 (Security Controls for the Authorised Business) and/or with SEC Appendix Z, Sections 6 and 7, the DCC shall ensure that its DCC Security Assessment response includes the matters referred to in Section G9.23.

G9.23 The matters referred to in this Section are that the DCC Security Assessment Response:

- (a) indicates whether the DCC accepts the relevant findings of the DCC Independent Security Assessment Service Provider and, where it does not, explains why this is the case;
- (b) sets out any steps that the DCC has taken or proposes to take in order to remedy and/or mitigate the actual or potential non-compliance or the increase in security risk (as the case may be) specified in the DCC Security Assessment Report; and
- (c) identifies a timetable within which the DCC proposes to take any such steps that have not already been taken.

G9.24 Where a DCC Security Assessment Response sets out any steps that the DCC proposes to take in accordance with Section G9.23(b), the Security Sub-Committee (having considered the advice of the DCC Independent Security Assessment Service Provider) shall review that response and either:

- (a) notify the DCC that it accepts that the steps that the DCC proposes to take, and the timetable within which it proposes to take them, are appropriate to remedy and/or mitigate the actual or potential non-compliance or increase in security risk (as the case may be) specified in the DCC Security Assessment Report; or
- (b) seek to agree with the DCC such alternative steps and/or timetable as would, in the opinion of the Security Sub-Committee, be more appropriate for that purpose.

G9.25 Where a DCC Security Assessment Response sets out any steps that the DCC proposes to take in accordance with Section G9.23(b), and where those steps and the timetable within which it proposes to take them are accepted by the Security Sub-Committee, or

alternative steps and/or an alternative timetable are agreed between it and the DCC in accordance with Section G9.24(b), the DCC shall:

- (a) take the steps that have been accepted or agreed (as the case may be) within the timetable that has been accepted or agreed (as the case may be); and
- (b) report to the Security Sub-Committee on:
  - (i) its progress in taking those steps, at any such intervals or by any such dates as the Security Sub-Committee may specify;
  - (ii) the completion of those steps in accordance with the timetable; and
  - (iii) any failure to complete any of those steps in accordance with the timetable, specifying the reasons for that failure.

#### Follow-up Security Assessment

G9.26 Where a DCC Security Assessment Response sets out any steps that the User proposes to take in accordance with Section G9.23(b), and where those steps and the timetable within which it proposes to take them are accepted by the Security Sub-Committee, or alternative steps and/or an alternative timetable are agreed between it and the User in accordance with Section G9.24(b), the DCC Independent Security Assessment Service Provider shall, at the request of the Security Sub-Committee (and by such date as it may specify), carry out a Follow-up Security Assessment of the DCC to:

- (a) identify the extent to which the DCC has taken the steps that have been accepted or agreed (as the case may be) within the timetable that has been accepted or agreed (as the case may be); and
- (b) assess any other matters related to the DCC Security Assessment Response that are specified by the Security Sub-Committee.

#### **DCC Security Assessments: Further Provisions**

G9.27 The DCC Independent Security Assessment Service Provider may, in carrying out any DCC Security Assessment, take into account any relevant security accreditation or certification held by the DCC.

### **Setting the Compliance Status**

G9.28 Following the completion of a Full DCC Security Assessment, the Security Sub-Committee shall consider the DCC Security Assessment Report and the DCC Security Assessment Response.

G9.29 The Security Sub-Committee shall identify whether any remaining non-compliances that exist with Section G2 or G4 to G6 and/or the DCC Licence Condition 8 (Security Controls for the Authorised Business) and/or SEC Appendix Z, Sections 6 and 7 and shall, where appropriate:

- (a) note and record that there are no non-compliances; or
- (b) note and record the specific non-compliances that need to be addressed.

G9.30 Where the Security Sub-Committee identifies remaining non-compliances that exist with Section G2 and G4 to G6 and/or the DCC Licence Condition 8 (Security Controls for the Authorised Business) and/or SEC Appendix Z Sections 6 and 7, it shall:

- (a) require the DCC to take the steps set out in Section G9.24: or
- (b) require a Follow-up Security Assessment as set out in Section G9.26.

G9.31 Where the Security Sub-Committee identifies any remaining non-compliances with Section G2 or G4 to G6 and/or the DCC Licence Condition 8 (Security Controls for the Authorised Business) and/or SEC Appendix Z, Sections 6 and 7, it shall notify the Panel as required by G9.37(b).

### **CPA Certificate Remedial Plan Preparation**

G9.32 The DCC shall ensure that it has in place (and periodically reviews) a policy for creating and managing compliance with CPA Certificate Remedial Plans. The DCC Independent Security Assessment Service Provider will assess the DCC's compliance with Appendix Z Section 6 and Section 7.

### **Disagreement with Security Sub-Committee Decisions**

G9.33 Where the DCC disagrees with any decision made by the Security Sub-Committee in relation to it under Section G9.28 to G9.31, it may appeal that decision to the Panel. If

the DCC disagrees with any decision made by the Panel, it may appeal that decision to the Authority and the determination of the Authority shall be final and binding for the purposes of the Code.

### **Events of Default**

G9.34 In relation to an Event of Default which consists of a material breach by the DCC of any of the obligations referred to at Section G9.2(c), the provisions of Sections M8.2 to M8.4 shall apply subject to the provisions of Sections G9.35 to G9.41.

G9.35 For the purposes of Sections M8.2 to M8.4 as they apply pursuant to Section G9.34, an Event of Default shall (notwithstanding the ordinary definition thereof) be deemed to have occurred in respect of the DCC where it is in material breach of any of the obligations referred to at Section G9.2(d) (provided that Sections M8.4(e), (f) and (g) shall never apply to the DCC).

G9.36 Where in accordance with Section M8.2 the Panel receives notification that the DCC is in material breach of any of the obligations referred to at Section G9.2(d), it shall refer the matter to the Security Sub-Committee.

G9.37 On any such referral the Security Sub-Committee may investigate the matter in accordance with Section M8.3 as if the references in that Section to the “Panel” were to the “Security Sub-Committee”.

G9.38 Where the Security Sub-Committee has:

- (a) carried out an investigation in accordance with Section M8.3; or
- (b) received a DCC Security Assessment Report concluding that the DCC is in actual or potential non-compliance with any of the obligations referred to at Section G9.2(c),

the Security Sub-Committee shall consider the information available to it and, where it considers that actual non-compliance with any of the obligations referred to at Section G9.2(c) has occurred, shall refer the matter to the Panel for it to determine whether that non-compliance constitutes an Event of Default.

G9.39 Where the Panel determines that an Event of Default has occurred, it shall:

#### Annex 4 - Revised legal drafting – SEC Section G

- (a) notify the DCC and any other Party it considers may have been affected by the Event of Default; and
- (b) determine the appropriate steps to take in accordance with Section M8.4.

G9.40 Where the Panel is considering what steps to take in accordance with Section M8.4, it may request and consider the advice of the Security Sub-Committee.

G9.41 Where the Panel determines that the DCC is required to give effect to a remedial action plan in accordance with Section M8.4(d) that plan must be approved by the Panel (having regard to any advice of the Security Sub-Committee).

#### **CPA Certificate Remedial Plan Preparation**

G9.42 The DCC shall ensure that it has in place (and periodically reviews) a policy for creating and managing compliance with CPA Certificate Remedial Plans.

**G12 Security Assurance of Device Triage Facilities**

G12.1 Some of the expressions used in this Section G12 are defined in Section G12.9.

G12.2 Where the SSC Guidance for Device Security Assurance and Triage specifies that independent assurance of Triage Facility Providers is required to achieve appropriate levels of security assurance in accordance with the requirements of this Code, this Section G12 shall apply.

**Triage Facility Provider Obligations**

G12.3 In order to become a Triage Facility Provider, an entity must either be an existing Party or accede to this Code and become a Party. A Triage Service Provider is not required to be a User.

G12.4 Each Triage Facility Provider shall:

- (a) not attempt to undertake Triage Activities on any Device where the tamper-protection boundary required by the CPA Security Characteristics has already been breached before reaching the Triage Facility (taking into account any allowable breaches necessary as part of essential Device maintenance and/or the de-commissioning process);
- (b) only use the Triage Tool and Triage System Interface provided by a Device's Manufacturer to access the Manufacturer's Triage System and not use any other electronic devices, interfaces or IT systems for carrying out Triage Activities;
- (c) ensure multi-factor authentication and role-based access controls are used within its Triage Facility to control access to the graphical user interface (GUI) of the Triage Tool, and to control access to the Triage System Interface;
- (d) at all times prevent unauthorised use of the Triage Tool and Triage System Interface, and ensure the physical security of the Triage Tool and any Devices that are subject to Triage Activities;
- (e) ensure that all the required tamper-protection seals are fitted to Devices on completing the Triage Activities;

Annex 4 - Revised legal drafting – SEC Section G

- (f) maintain an asset management system to record Triage Activities undertaken at the Triage Provider's Triage Facility, including details of:
  - (i) the Requestor of any change to the configuration of a Device;
  - (ii) the Device Model and serial number of each Device where the tamper-protection boundary is breached in order to undertake (or attempt to undertake) Triage Activities;
  - (iii) details of Triage Activities successfully undertaken;
  - (iv) details of any failed attempts to complete Triage Activities; and
  - (v) confirmation that any seals and tamper-protection required by the CPA Security Characteristics have been applied before returning a Device to a Requestor;
- (g) when requested by the Security Sub-Committee, provide the Security Sub-Committee with an up-to-date copy of the records maintained pursuant to Section G12.3(f);
- (h) provide all reasonable assistance that may be requested by the Security Sub-Committee or the User Independent Security Assurance Service Provider for the purposes of conducting a User Security Assessment;
- (i) subject to Section G12.5, comply with the requirements of Sections G1, G3 to G5, G7 and G8;
- (j) comply with the requirements of Sections G12.6 to G12.8; and
- (k) act in accordance with Good Industry Practice.

G12.5 For the purposes of Sections G1, G3 to G5, G7 and G8, unless the SSC Guidance for Device Security Assurance and Triage states otherwise, a Triage Facility Provider shall be treated as if it is a User and:

- (a) any reference to a 'User' shall be deemed to include a reference to a 'Triage Facility Provider';

- (b) except for where the SSC Guidance for Device Security Assurance and Triage states otherwise, obligations in those Sections which are expressed to apply to a User shall apply to a Triage Facility Provider;
- (c) references in those obligations to 'User Systems' shall be deemed, for the purpose of their application to the Triage Facility Provider, to be references to the Triage Activities undertaken at the Triage Facility; and
- (d) the Security Sub-Committee shall provide Triage Facility Providers and other Parties with guidance on interpretation of Sections G1, G3 to G5, G7 and G8 in respect of their application to Triage Facility Providers and Triage Activities.

### **User Security Assessments of Triage Facilities**

G12.6 Prior to undertaking any Triage Activities, each Triage Facility Provider shall be subject to an initial Full User Security Assessment by a User Independent Security Assurance Service Provider following the process in Sections G8.22 to G8.30.

### **Approval**

G12.7 On receipt of the initial Full User Security Assessment Report and the User Security Assessment Response, the assurance status shall be set in accordance with Sections G8.35 to G8.36 and:

- (a) where the assurance status is set to 'approved' under Section G8.36(a) then the Triage Facility Provider may undertake Triage Activities as set out in the SSC Guidance for Device Security Assurance and Triage;
- (b) where the assurance status is set to 'approved' subject to conditions (as set under Section G8.36(b)) then the Triage Facility Provider will require explicit approval from the Security Sub-Committee before undertaking Triage Activities; and
- (c) where the assurance status is 'deferred' or 'rejected' under Section G8.36(c) or (d), respectively, then the Triage Facility Provider is not approved to undertake Triage Activities.

### **Second and subsequent User Security Assessments**

G12.8 Within 12 months following completion of the initial and each subsequent User Security Assessment, the Triage Facility Provider shall schedule a subsequent User Security Assessment with the User Independent Security Assurance Provider. The Security Sub-Committee shall determine the category of each such User Security Assessment to be carried out and, in doing so shall:

- (a) consider any security risks identified during or since the previous User Security Assessment;
- (b) take account of the volume of Devices for which Triage Activities are carried out; and
- (c) reach a determination based on a proportionate assessment of the security risks as to whether the next User Security Assessment should be:
  - (i) a Full User Security Assessment;
  - (ii) a Verification User Security Assessment; or
  - (iii) a User Security Self-Assessment.

### Definitions

G12.9 For the purpose of this Section G12:

|                                                              |                                                                                                                                                                                                                                                                                |
|--------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Requestor</b>                                             | means an entity (such as a Party or a meter asset provider) that requests that Triage Activities are undertaken by a Triage Facility Provider.                                                                                                                                 |
| <b>SSC Guidance for Device Security Assurance and Triage</b> | means the documents published by the Security Sub-Committee under Section G7.19(gi), which sets out guidance on the requirements and processes (including security controls and security assurance) to be followed by Triage Facility Providers undertaking Triage Activities. |
| <b>Triage</b>                                                | means the diagnosis, upgrading or resetting of a                                                                                                                                                                                                                               |

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                 | Device.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Triage Activities</b>        | <p>means any Triage-related activity carried out in circumstances where the SSC Guidance for Device Security Assurance and Triage requires independent assurance, including in such circumstances:</p> <ul style="list-style-type: none"> <li>a) the breach of the tamper-protection boundary;</li> <li>b) any unlocking of internal non-operational ports;</li> <li>c) any changes to the configuration of the Device Data;</li> <li>d) confirmation of the firmware version on the Device when Triage has been completed; and</li> <li>e) completion of Triage by replacing all internal non-operational port seals required pursuant to the CPA Security Characteristics and all tamper protection boundary seals.</li> </ul> |
| <b>Triage Facility</b>          | means a premises where Triage Activities are undertaken.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Triage Facility Provider</b> | means a Party which operates a Triage Facility for the purpose of carrying out Triage Activities.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Triage System Interface</b>  | means a secure IPsec virtual private network, site to site encrypted link provided by a Manufacturer in order to connect its Triage System to a Triage Tool at a Triage Facility, which provides confidentiality and integrity of communications.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |

Annex 4 - Revised legal drafting – SEC Section G

|                      |                                                                                                                                                                                                                                                                                                                                                                                                                       |
|----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Triage System</b> | means a secure IT system established for the purposes of Triage and operated by a Manufacturer, as part of its Device manufacturing capability, which the Triage Facility Provider connects to using the Triage Tool and Triage System Interface, and which is compliant with the requirements of the <a href="#">NCSC Commercial Product Assurance (CPA)</a> Scheme and the associated CPA Security Characteristics. |
| <b>Triage Tool</b>   | means an electronic device provided by a Manufacturer, which is used to Triage Devices in accordance with SSC Guidance for Device Security Assurance and Triage, and which is cryptographically authorised such that it can only be used for Triage Activities and cannot be given additional capabilities by an operator in a Triage Facility.                                                                       |

## G13 The CPA Scheme Operator

### Procurement of the CPA Scheme Operator

G13.1 The Security Sub-Committee, subject to the approval of the Panel, shall procure the provision of services in relation to the operation of the CPA Scheme:

- (a) of the scope specified in Section G13.3;
  - (b) from a person who:
    - (i) is suitably qualified in accordance with Section G13.4; and
    - (ii) is suitably independent in accordance with Section G13.5,
- and that person is referred to in this Section G13 as the “CPA Scheme Operator”.

G13.2 The Security Sub-Committee may appoint more than one person to carry out the functions of the CPA Scheme Operator.

### Scope of CPA Scheme Operator Services

G13.3 The services specified in this Section G13.3 (the "CPA Scheme Operator Services") are services in accordance with which the CPA Scheme Operator shall:

- (a) develop a standard form of contract – which shall require to be approved by the Security Sub-Committee (and following such approval shall be known as the "CPA Test Lab Framework Agreement") – to be entered into by each CPA Test Lab in relation to the performance of its functions for the purposes of the CPA Scheme, and which shall in particular:
  - (i) require that the CPA Test Lab comply with all applicable provisions of the CPA Policies and Procedures (as amended from time to time), including in particular those which:
    - (A) set out the criteria to be satisfied in order to perform the functions of a CPA Test Lab for the purposes of the CPA Scheme; and
    - (B) describe the procedures to be applied in evaluating whether a

Device Model should be issued with a CPA Certificate; and

- (ii) constitute an agreement under which the CPA Scheme Operator shall be entitled, on behalf of any Manufacturer, to receive services provided by the CPA Test Lab for the purposes of evaluating whether any Device Model should be issued with a CPA Certificate;
- (b) develop a standard form of contract – which shall require to be approved by the Security Sub-Committee (and following such approval shall be known as the "CPA Manufacturer Standard Agreement") – to be entered into by any Manufacturer seeking to obtain and maintain a CPA Certificate in relation to a Device Model, and which shall in particular provide that the Manufacturer:
  - (i) must comply with all applicable provisions of the CPA Policies and Procedures (as amended from time to time); and
  - (ii) may obtain the services of a CPA Test Lab for the purposes of the CPA Scheme only via the CPA Scheme Operator, under and in accordance with terms specified in the agreement;
- (c) enter into the CPA Test Lab Framework Agreement and CPA Manufacturer Standard Agreement with relevant CPA Test Labs and Manufacturers;
- (d) issue CPA Certificates to Manufacturers in relation to Device Models which have been successfully demonstrated to satisfy the requirements of the CPA Security Characteristics;
- (e) renew, suspend, withdraw or cancel CPA Certificates in such circumstances as may from time to time be described in the CPA Policies and Procedures;
- (f) carry out such evaluation (and related) functions as may from time to time be set out in the CPA Policies and Procedures, or which it is otherwise requested by the Security Sub-Committee to carry out, which may include in particular:
  - (i) assessing, and from time to time reviewing, whether a Test Lab which wishes to perform the functions of a CPA Test Lab meets the criteria specified for that purpose in the CPA Policies and Procedures;

Annex 4 - Revised legal drafting – SEC Section G

- (ii) where a Test Lab does not meet the criteria specified in the CPA Policies and Procedures for performing the functions of a CPA Test Lab, advising on the reasons for the failure and the changes or additional evidence that would be needed in order for it to meet those criteria;
  - (iii) responding to technical enquiries from Manufacturers and CPA Test Labs in relation to the evaluation process for Device Models in respect of which a CPA Certificate is being (or is proposed to be) sought (the "**evaluation process**");
  - (iv) reviewing and approving the proposed testing regime in respect of any Device Model for which a CPA Certificate is being sought;
  - (v) reviewing the results of tests carried out by a CPA Test Lab in relation to a Device Model for which a CPA Certificate is being sought, in order to:
    - (A) determine whether a CPA Certificate should be issued in respect of that Device Model; and
    - (B) where a Device Model has not satisfied the requirements for the issue of a CPA Certificate, advising on the reasons for the failure and the changes or additional evidence that would be needed in order for it to be issued with a CPA Certificate;
  - (vi) liaising with, and providing information and support to, CPA Test Labs and Manufacturers in relation to the evaluation process; and
  - (vii) providing such information and advice to the Security Sub-Committee as may be requested from time to time;
- (g) oversee the interactions between Manufacturers and CPA Test Labs in relation to the evaluation process;
- (h) provide information, advice and support to any Test Lab which wishes to perform the functions of a CPA Test Lab for the purposes of the CPA Scheme;
- (i) attend meetings of the Security Sub-Committee whenever requested to do so by

the Security Sub-Committee Chair for the purpose of providing advice and information, and otherwise delivering such reports or presentations, as may be requested;

(j) provide such written reports, advice and information to the Security Sub-Committee, in relation to the operation of the CPA Scheme and the provision of the CPA Scheme Operator Services, as it may from time to time request;

(k) provide such other support and assistance to the Security Sub-Committee as it may from time to time request; and

(l) undertake such other activities, and do so at such times and in such manner, as may be further provided for in this Section G13.

#### **Suitably Qualified Person**

G13.4 The CPA Scheme Operator shall be treated as suitably qualified in accordance with this Section G13.4 only if it satisfies such requirements as to its qualifications as the Security Sub-Committee may from time to time determine for the purposes of the process of procuring services in relation to the operation of the CPA Scheme.

#### **Independence Requirement**

G13.5 The CPA Scheme Operator shall be treated as suitably independent in accordance with this Section G13.5 only if it satisfies:

(a) the requirements specified in Section G13.7; and

(b) the requirements specified in Section G13.8.

G13.6 For the purposes of Sections G13.7 and G13.8:

(a) a "**Relevant Person**" means any of the following:

(i) the DCC;

(ii) a DCC User;

(iii) the owner or operator of any Test Lab which performs the functions of a CPA Test Lab for the purposes of the CPA Scheme;

(iv) the Manufacturer of any Device which requires a CPA Certificate;

(b) a "Relevant Service Provider" means any service provider to a Relevant Person from which that Relevant Person acquires capability for a purpose related to the CPA Scheme.

G13.7 The requirements specified in this Section G13.7 are that:

(a) no Relevant Person or any of its subsidiaries, and no Relevant Service Provider or any of its subsidiaries, holds or acquires any investment by way of shares, securities or other financial rights or interests in the CPA Scheme Operator;

(b) no director of any Relevant Person, and no director of any Relevant Service Provider, is or becomes a director or employee of, or holds or acquires any investment by way of shares, securities or other financial rights or interests in, the CPA Scheme Operator; and

(c) the CPA Scheme Operator does not hold or acquire a participating interest (as defined in section 421A of the Financial Services and Markets Act 2000) in any Relevant Person or any Relevant Service Provider,

(but for these purposes references to a Relevant Service Provider shall not include the CPA Scheme Operator where it acts in that capacity).

G13.8 The requirements specified in this Section G13.8 are that the CPA Scheme Operator is able to demonstrate to the satisfaction of the Security Sub-Committee that it:

(a) has in place arrangements to ensure that it will at all times act independently of any commercial relationship that it has, has had, or may in future have with a Relevant Person or Relevant Service Provider (and for these purposes a 'commercial relationship' shall include a relationship established by virtue of the CPA Scheme Operator itself being a Relevant Service Provider to any Relevant Person); and

(b) satisfies such other requirements as to its independence as the Security Sub-Committee may from time to time determine for the purposes of the process of procuring services in relation to the operation of the CPA Scheme.

**Compliance of the CPA Scheme Operator**

G13.9 The Security Sub-Committee shall be responsible for ensuring that the CPA Scheme Operator provides the CPA Scheme Operator Services, and carries out its functions as such, in accordance with the provisions of this Section G13.

## **G14 The CPA Transition Approach Document**

### **Overview**

G14.1 The CPA Transition Approach Document is to be developed by the Secretary of State and incorporated into this Code pursuant to Part G of Condition 22 of the DCC Licence and Section X5 (Incorporation of Certain Documents into this Code).

### **Purpose of the CPA Transition Approach Document**

G14.2 The purpose of the CPA Transition Approach Document is to:

- (a) provide that the Revised CPA Arrangements shall not have full effect immediately;
- (b) enable the gradual implementation of and transition to the Revised CPA Arrangements; and
- (c) provide for additional and/or varied provisions to apply for a transitional period to manage the interactions between the Revised CPA Arrangements and the previous arrangements for the CPA Scheme.

### **Content of the CPA Transition Approach Document**

G14.3 The CPA Transition Approach Document may include, without limitation, some or all of the following:

- (a) a modification process which enables the Security Sub-Committee to modify the CPA Transition Approach Document;
- (b) rights and/or obligations of the DCC and other Parties designed to facilitate or achieve the purposes of the CPA Transition Approach Document which are either additional to or vary other rights and/or obligations set out in this Code;
- (c) variations to the powers and/or duties of the Panel, the Security Sub-Committee and/or any other Sub-Committee designed to facilitate or achieve the purposes of the CPA Transition Approach Document which are either additional to or vary other powers and/or duties set out in this Code;

- (d) variations to the processes by which CPA Testing is administered, managed and/or operated, which may include variations to the requirements which apply to CPA Test Labs and/or Manufacturers;
- (e) mechanisms for completion or in-flight transfer of Device Models that are undergoing testing as part of the arrangements for the CPA Scheme which existed prior to the Revised CPA Arrangements;
- (f) pre-conditions that may need to apply prior to some or all of the Revised CPA Arrangements coming into effect;
- (g) variations in the arrangements for issuing of CPA Certificates, and/or the addition or removal of Device Models to or from the Certified Products List;
- (h) limitations and/or variations to the rights and/or obligations of the Parties to apply for a transitional period prior to the full implementation of the Revised CPA Arrangements;
- (i) provision for the referral and determination of disputes in respect of the CPA Transition Approach Document, which may include interim or final determinations by the Secretary of State, the Authority, the Security Sub-Committee, the Panel or any other person specified by the Secretary of State; and
- (j) a date from which the CPA Transition Approach Document shall cease to have effect, or a mechanism for determining such date.

#### **Definitions**

G14.4 For the purposes of this Section G14:

|                                        |                                                                                                                                                                                                                                                          |
|----------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b><u>Revised CPA Arrangements</u></b> | <u>means the modifications made to this Code, including in particular the addition to this Code of Section G13 (The CPA Scheme Operator), in order to incorporate into this Code provisions for the administration and governance of the CPA Scheme.</u> |
|----------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

